Cisco

La sécurité des réseaux

Vincent REMAZEILLES

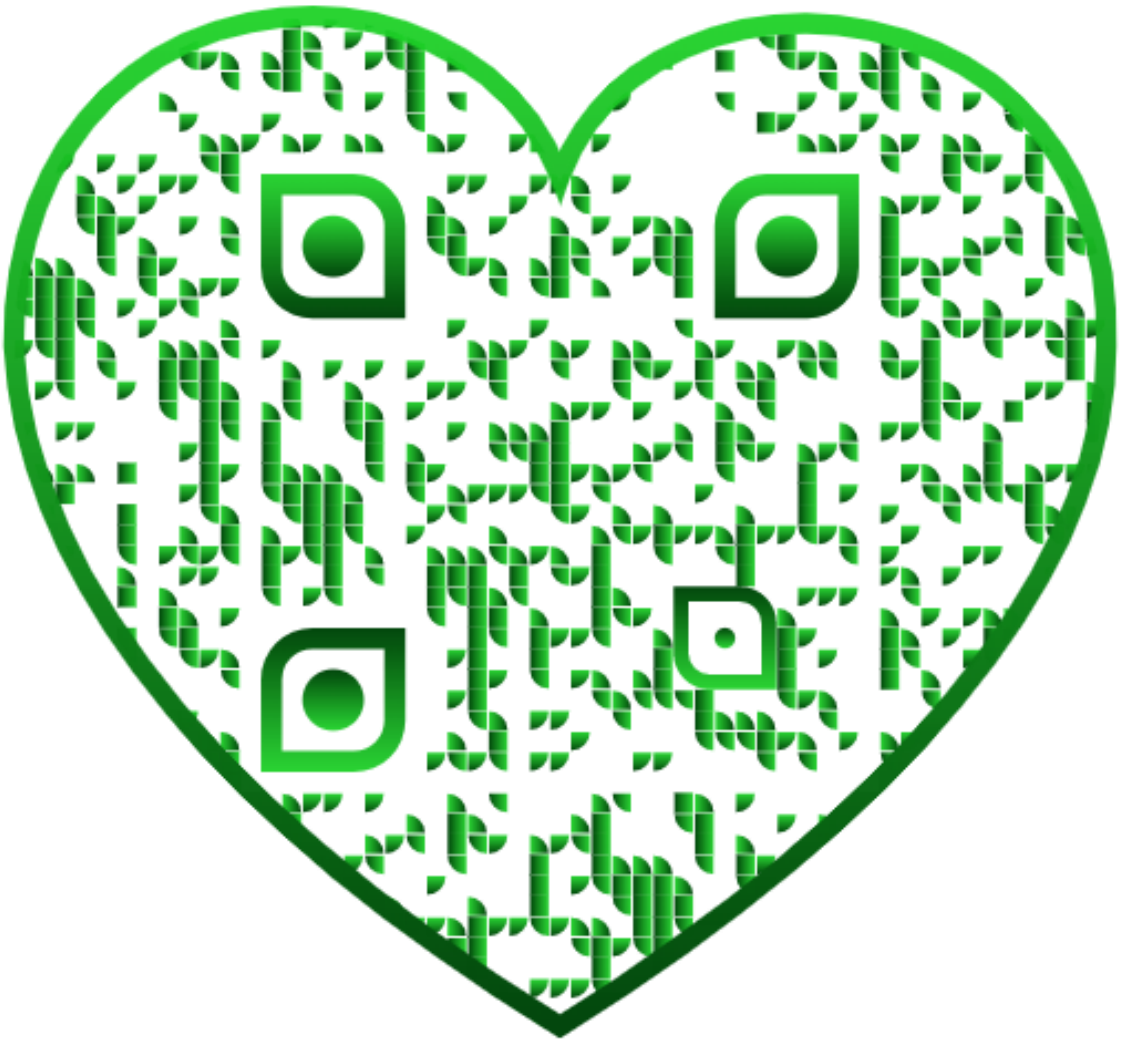
Résumé

Ce livre sur la sécurité des réseaux avec CISCO s'adresse aux **administrateurs réseaux** désireux d'améliorer la sécurité de leur domaine et aussi aux étudiants déjà familiers de la gamme du constructeur.
Des célèbres **Access-lists** aux dernières innovations en matière **d'analyse protocolaire** et de **VPN SSL**, en passant par la **sécurité des réseaux sans fil**, ce livre propose un tour d'horizon de ce qu'il est possible d'entreprendre pour protéger efficacement son réseau en exploitant au mieux les possibilités offertes par les équipements couramment utilisés par les entreprises.
Le thème de la sécurité est dans un premier temps abordé en opérant une correspondance avec les couches du **modèle OSI** avant d'être examiné dans le détail avec les configurations propres aux **points d'accès Wi-Fi**, aux **routeurs**, aux **commutateurs** Ethernet et aux **pare-feux**.
Les problématiques de sécurité autour de la **téléphonie sur IP** font quant à elles l'objet d'un chapitre dans lequel sont également développées les mesures permettant de préserver la confidentialité des communications grâce à la **cryptographie**.
Le livre se veut **didactique** et présente les réflexions préalables à la construction d'une **infrastructure sécurisée** ainsi que les configurations des équipements, illustrées avec les innombrables possibilités de la **ligne de commande Cisco**.

L'auteur

Vincent Remazeilles est Ingénieur Réseau et Sécurité, titulaire d'un DESS Sécurité des SI. Il effectue différentes missions en tant que consultant Senior dans le domaine de la sécurité auprès de grands comptes industriels. A travers ce livre, le lecteur bénéficie de toute son expertise et expérience dans le domaine de la sécurité et des équipements Cisco

Ce livre numérique a été conçu et est diffusé dans le respect des droits d'auteur. Toutes les marques citées ont été déposées par leur éditeur respectif. La loi du 11 Mars 1957 n'autorisant aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les "copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective", et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, "toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayant cause, est illicite" (alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal. Copyright Editions ENI



Introduction

Ce livre est destiné à un public qui possède quelques notions sur la configuration des équipements de la gamme Cisco en ligne de commande ainsi qu'en réseaux IP. L'objectif de ce livre est de donner au lecteur une vue sur les possibilités offertes par Cisco sur les routeurs, les commutateurs Ethernet et les pare-feu les plus communément rencontrés dans les entreprises. Il est question ici de tirer le meilleur parti de ces équipements dans le domaine de la sécurité avec des manipulations aisément compréhensibles.

Nous aborderons la sécurité des réseaux de données en nous référant aux couches du modèle OSI. Cette approche a l'avantage de faciliter la compréhension des diverses techniques mises en œuvre et aide grandement lorsqu'il s'agit de se pencher au chevet d'un réseau en panne.

Les extraits de configuration et les exemples qui illustrent les chapitres de ce livre sont en grande partie issus de la ligne de commande (CLI (*Command Line Interface*)), ce choix est motivé par une grande régularité de celle-ci contrairement aux interfaces graphiques qui sont en perpétuelle évolution.

Au-delà des couches du modèle OSI, nous avons fait le choix de mettre en avant les pare-feu et la sécurité de la téléphonie sur IP en leur consacrant deux chapitres.

© ENI Editions - All rigths reserved - Moha Anisa

Structure du livre

Le chapitre "La sécurité des couches une et deux" est consacré aux deux premières couches du modèle OSI. Ces deux couches basses très proches du média physique sont la porte d'entrée dans le système d'exploitation des équipements ou des hôtes d'un réseau. Nous aborderons dans ce chapitre la protection de la couche physique contre les tentatives d'accès. Quant à la couche 2, elle est la cible de nombreuses attaques visant à s'introduire frauduleusement sur les réseaux en usurpant l'identité d'un hôte qui s'y trouve déjà. Nous aborderons également le sujet de l'authentification préalable à toute connexion sur le réseau.

Le chapitre "La sécurité de la couche réseau" est dédié aux couches réseau et transport du modèle OSI. C'est l'univers du protocole TCP/IP qui est le mode de communication du réseau Internet et des réseaux d'entreprise. Les réseaux, si aucune mesure n'est prise, communiquent naturellement entre eux et les mesures de protection abordées dans ce chapitre introduisent les listes de filtrage d'accès destinées à limiter les communications lorsque le besoin s'en fait sentir. Les communications qui utilisent TCP/IP nécessitent parfois une protection contre les écoutes afin de préserver un niveau élevé de confidentialité. Nous présenterons dans ce chapitre une manière de sécuriser les communications intersites avec IPSec.

Le chapitre "La sécurité des réseaux sans fil" aborde les problématiques liées au réseaux sans fil communément désignés par le nom de Wi-Fi. Ces réseaux utilisent les ondes radio pour interconnecter les clients au réseau filaire. Tout comme pour TCP/IP, si rien n'est entrepris, les points d'accès sans fils peuvent tout à fait offrir leurs services au premier venu ce qui n'est pas souhaitable. Nous aborderons les méthodes d'accès sécurisées et les mesures simples qui permettent de limiter la portée des ondes radio tout en offrant un service de qualité.

Le chapitre "Notions d'architecture réseau sécurisée" traite des notions d'architecture réseau toujours sous le prisme de la sécurité. Cisco recommande un modèle réseau découpé en zones qui favorise l'application de règles de sécurité en fonction de la protection nécessitée par la zone. Ce découpage correspond aussi à celui des zones fonctionnelles de l'entreprise comme nous le verrons. Nous aborderons les relations entre ces diverses zones et le sens particulier des flux entre elles. L'architecture revêt de par les études qu'elle génère une grande importance pour la consistance d'un réseau.

Le chapitre "La protection des équipements" introduit l'absolue nécessité de porter une grande attention à la protection des équipements qui constituent l'ossature du réseau. Sans une protection adéquate des équipements ceux-ci sont exposés aux attaques mais aussi aux erreurs de manipulation. La protection des journaux est aussi évoquée.

Le chapitre "Sécurité de la téléphonie sur IP" est consacré à la sécurité de la téléphonie sur IP qui fait partie de notre quotidien professionnel et personnel. Nous constaterons que cette technologie en tant qu'application en réseau hérite des problèmes de sécurité de toutes les couches du modèle OSI. La téléphonie sur IP pour la protection des conversations et de la signalisation fait largement appel à la cryptographie. Les fonctions de filtrage sur la signalisation permettent d'entraver les tentatives de fraudes.

Le chapitre "Firewalls" est entièrement consacré aux pare-feu et tout particulièrement au modèle phare de Cisco, le modèle ASA. Ce chapitre comporte des descriptions des fonctions telles que les listes de sécurités ou ACL, la création des zones démilitarisées (ou DMZ) et la Traduction d'Adresses Réseau. Une partie est consacrée à la téléphonie sur IP ainsi qu'aux VPN SSL qui constituent un moyen d'accès sécurisé pour les utilisateurs nomades.

© ENI Editions - All rigths reserved - Moha Anisa

La politique de sécurité réseau

C'est une expression, un concept parfois un peu flou dont on entend parler lorsqu'il devient nécessaire de s'organiser. Qu'est-ce qu'une politique de sécurité ? En avons-nous besoin ? La réponse est oui.

Une politique de sécurité est un document dans lequel se trouvent (s'il est bien élaboré) toutes les réponses aux questions qu'un ingénieur en charge d'une étude se pose lorsqu'il aborde le volet sécurité d'un projet informatique dont la réussite dépend entre autres de la prise en compte dès le début des contraintes de sécurité. (Nous parlons aussi d'exigences). Une politique de sécurité est donc un document confidentiel (largement diffusé toutefois) qui en faisant abstraction des contingences matérielles et techniques fournit une collection de directives de sécurité classées par thèmes. La mise en pratique de la politique de sécurité est l'application des directives aux thèmes couverts par le projet.

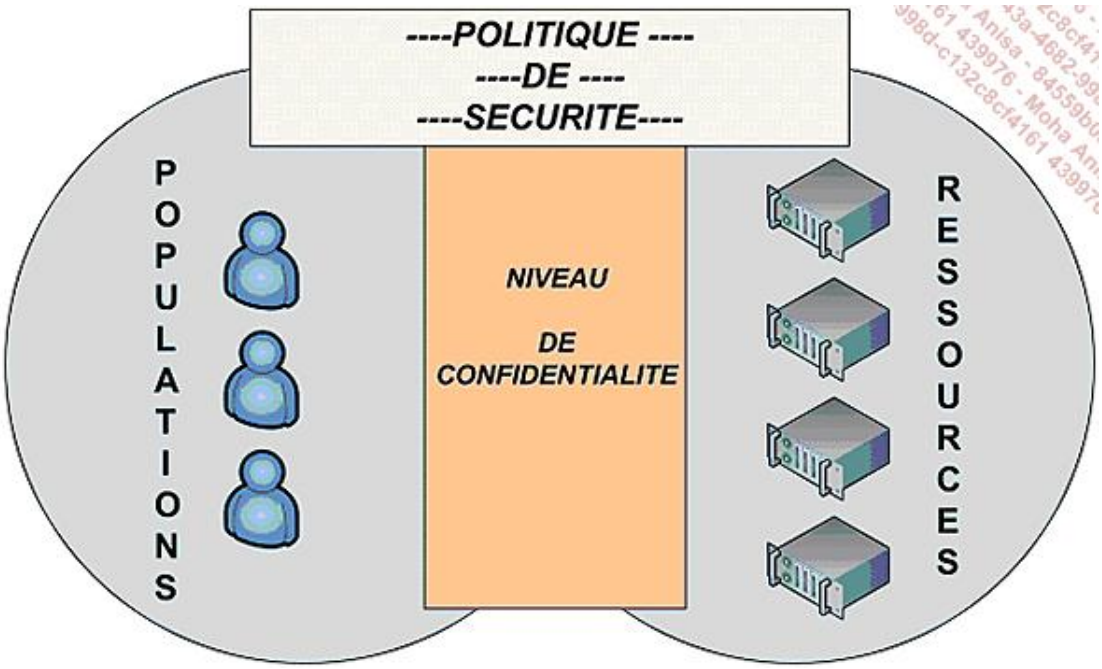
La thématique réseau dans la politique de sécurité englobe les recommandations pour l'exploitation des liens réseaux et des équipements. Les domaines abordés évoluent avec les intérêts économiques de l'entreprise et concernent entre autres :

- la gestion des accès au réseau et aux ressources (en relation avec la gestion des identités et des droits) ;
- la cryptographie ;
- la sécurité des équipements et des configurations ;
- la sécurité des systèmes terminaux.

Cependant, il serait illusoire et coûteux de vouloir à tout prix protéger l'entièreté d'une infrastructure informatique à la manière d'un Fort Knox. C'est pourquoi, la politique de sécurité s'applique à des degrés divers aux réseaux et aux équipements en fonction du niveau de confidentialité entre les populations et les ressources.

La conception de la politique de sécurité débute donc avec une classification du niveau de confidentialité des ressources et d'habilitation des populations. En fonction de cette classification, des règles sont émises et écrites dans le document. Ce travail est fastidieux mais ne revêt pas un caractère obligatoire. Il est envisageable de tout classifier à un niveau unique et ainsi de simplifier la politique de sécurité.

Le schéma suivant illustre cette notion.



Considérons un exemple simple :

Une population reçoit une habilitation de niveau *confidentiel*. Un ensemble de documents est également classé *confidentiel*.

La politique de sécurité indique :

© ENI Editions - All rigths reserved - Moha Anisa

- l'accès à des documents classés *confidentiel* n'est autorisé qu'aux personnels disposant d'une habilitation à ce niveau ou à un niveau supérieur ;

- la durée d'utilisation des documents classés de type *confidentiel* est enregistrée ;

- les documents classés *confidentiel* sont uniquement accessibles en lecture seule ;

- les documents classés *confidentiel* sont consultables à distance uniquement au travers d'un canal chiffré sur les réseaux de type LAN ou WAN.

Cet exemple illustre la relation entre une population, une ressource, un niveau de confidentialité et la politique de sécurité. Cette approche est primordiale dans la mesure où les réseaux d'entreprise ne sont plus limités à leurs frontières traditionnelles mais s'étendent vers les réseaux de leurs partenaires tout en recevant les connexions des employés en déplacement et couramment désignés comme "nomades".

Ces règles sont au-dessus de toute contingence technique. Une obligation de chiffrer les communications sur une liaison n'indique pas obligatoirement quel type de chiffrement sera utilisé dans la mesure où les techniques évoluent en permanence. Malgré tout, il est envisageable de le préciser à condition de veiller à la mise à jour périodique du document.

Complétons l'exemple précédent :

... au travers d'un canal chiffré sur les réseaux de type LAN ou WAN. Chiffrement en AES 256 sur les équipements du réseau avec authentification par certificats. Il est également possible, en complément de cette précision, que la mise en œuvre du chiffrement relève d'une autre documentation définissant les standards en vigueur pour le déploiement. Enfin, la documentation technique précise la manière dont le protocole est configuré sur les équipements du réseau.

La rédaction d'une politique de sécurité est un travail sur mesure dont le document final est applicable à toutes les ressources et à toutes les populations de l'entreprise. Ce document est obligatoirement validé au plus haut niveau de la hiérarchie. Il est important de faire évoluer la politique de sécurité en fonction des liens qui ne manquent pas de se tisser avec les partenaires et les clients. Une politique qui n'évolue pas perd tout son sens et devient peu à peu inapplicable. La littérature anglo-saxonne reprend à l'infini le concept du docteur DEMING « Plan, Do, Check, Act » ce qui dans notre langue se traduit par planifier, faire, vérifier, corriger. Ceci s'applique tout à fait à la politique de sécurité et constitue un véritable cycle d'évolution permanente.

La rédaction de la politique de sécurité n'en est pas pour autant une affaire de spécialistes extérieurs. Dans l'entreprise, il est recommandé de créer un groupe de travail autour de la rédaction de ce document.

© ENI Editions - All rigths reserved - Moha Anisa

Terminologie

Nous allons brièvement évoquer les quelques mots-clés qui sont largement repris dans la littérature informatique lorsque la sécurité est abordée.

Une *vulnérabilité* est une faiblesse le plus souvent cachée touchant une infrastructure informatique. Ce terme est fréquemment associé aux logiciels mais il regroupe plus généralement toute faiblesse quelle qu'en soit la nature. Une erreur de configuration d'un équipement réseau constitue une vulnérabilité tout comme un mot de passe vide ou trivial. L'expression faille de sécurité est également employée. Les moyens et les méthodes visant à éliminer les vulnérabilités sont faciles à mettre en pratique et requièrent :

- de se tenir au courant des vulnérabilités auprès du constructeur ;
- d'opérer une veille technologique à partir de sites Internet dédiés à la sécurité informatique ;
- de tester sur un environnement de validation les correctifs publiés ;
- de tester une procédure de retour en arrière ;
- d'installer le correctif ;
- d'observer le comportement de l'infrastructure de production.

Un *risque* est la probabilité qu'un problème survienne lorsqu'une vulnérabilité est exposée à une population malveillante qui tentera de l'exploiter. Il existe d'autres définitions selon la norme à laquelle on se réfère. L'objectif de la sécurité informatique est de diminuer le plus possible le risque par tous les moyens disponibles.

Exploiter une vulnérabilité revient à utiliser cette faiblesse pour mettre à mal le dispositif visé par l'attaque. Concrètement, un exploit est un petit programme qui est lancé en direction de l'adresse réseau du système visé. Les équipements et les architectures informatiques comportent parfois de multiples vulnérabilités qui ne sont jamais révélées publiquement et ne sont donc jamais corrigées, en revanche les individus qui les ont découvertes les exploitent à leur guise pour leur propre compte.

Mettre à jour un système ou un équipement réseau consiste à appliquer les correctifs publiés par le constructeur et faisant suite à la révélation d'une vulnérabilité. En la matière, la prudence s'impose et avec elle toutes les séries de tests nécessaires afin de vérifier le bon fonctionnement de l'ensemble concerné une fois que les correctifs ont été appliqués. Quoi qu'il en soit, un suivi régulier des publications, des correctifs et des retours d'expérience sont fortement recommandés.

La politique de sécurité est élaborée en fonction d'une variable connue sous le nom d'environnement. L'environnement dans le domaine de la sécurité informatique est la définition de l'univers dans lequel évolue un système d'information. L'environnement, dans le domaine de la sécurité établit une carte des menaces potentielles qui planent sur un système d'information. Il s'agit au final de déterminer la portée de la politique de sécurité en fonction des menaces dont l'entreprise souhaite se prémunir. Par exemple, une entreprise décide d'instaurer des mesures de protection contre les menaces les plus courantes (et d'y consacrer un certain budget) mais décide de ne pas traiter les menaces émanant d'agences gouvernementales. La variable d'environnement est donc utilisée pour régler le degré de protection de la politique de sécurité face à une catégorie de menaces.

© ENI Editions - All rigths reserved - Moha Anisa

Cycle de la politique de sécurité

Comme nous l'avons évoqué, la politique de sécurité suit un cycle connu le nom de cycle de DEMING. Parcourons-en les phases.

1. La planification (Plan...)

La planification commence avec la décision d'organiser formellement la sécurité. Elle consiste en un inventaire exhaustif des ressources à protéger et à la rédaction de directives pour chaque domaine concerné. À la fin de cette phase de planification, la politique de sécurité sera rédigée par le groupe de travail avec l'assistance éventuelle d'un consultant ayant une vue extérieure sur l'entreprise et son projet. Une fois écrite et relue, elle doit absolument être validée par la plus haute autorité afin qu'aucune contestation ne soit possible quant à son cadre d'application. L'étape suivante est sa publication sous la forme d'un document confidentiel mais facilement accessible. Sa publication va de pair avec une large diffusion auprès des équipes en charge des projets et de l'exploitation de l'infrastructure informatique. Il est primordial d'inclure les contraintes de sécurité dès les premières phases qui jalonnent le déroulement d'un projet afin de ne pas risquer de l'interrompre s'il venait à prendre une voie contraire à la politique de sécurité en vigueur.

La politique de sécurité est déclinée en domaines fonctionnels qui représentent le modèle du système d'information de l'entreprise. Son organisation prend la forme de chapitres au sein desquels figurent les points à respecter. Citons par exemple, le chapitre sur la sécurité des systèmes d'exploitation, la sécurité des bases de données et la sécurité des communications qui nous intéresse au premier chef. Les divers intervenants lors de la phase de planification devront toujours avoir à l'esprit que leur texte servira de base aux travaux de sécurisation qui ne manqueront pas de se succéder. Ainsi la clarté et la précision des propos sont de mise lors de l'élaboration de la politique de sécurité.

2. La mise en œuvre (Do...)

La mise en œuvre de la politique de sécurité correspond point pour point à ce que nous venons de décrire précédemment. L'adhésion de tous au respect des règles décrites est le fondement d'une bonne prise en compte de la sécurité.

La politique de sécurité est principalement mise en œuvre lors des premières phases de progression d'un projet quel qu'il soit. Ce livre se cantonne à la sécurité des réseaux, mais le champ d'application de la politique de sécurité est vaste. La politique de sécurité est une référence qui doit être introduite dans chaque activité en relation avec le système d'information. À titre d'exemple, un projet partant d'une feuille blanche ou visant à modifier une partie de l'architecture doit impérativement se référer à la politique de sécurité. Ainsi, les spécifications techniques reprennent toutes les références utiles de la politique de sécurité afin de les intégrer naturellement. L'expérience montre que la sécurité si elle n'est pas prise en compte dès les prémices d'un projet peine par la suite à s'y intégrer. C'est la raison pour laquelle la diffusion de la politique de sécurité doit viser un large public et il est bon que chaque responsable de secteur (base de données, développement, réseaux) maîtrise la partie qui le concerne.

3. Le suivi (Check...)

Le suivi de la politique de sécurité consiste à s'assurer que les contraintes imposées par le texte sont prises en compte par les équipes en charge des projets et celles en charge de l'exploitation. Cela implique une présence systématique d'un représentant ou responsable de la sécurité aux réunions de suivi et un contrôle des processus d'exploitation en vigueur. Les menaces et les techniques évoluent perpétuellement et une politique de sécurité en aucun cas ne saurait rester figée. Le risque étant qu'elle ne soit tout simplement plus appliquée. Cette approche concerne donc le suivi de l'application de la politique de sécurité

L'évolution de la politique est donc prise en compte dès sa définition par l'élaboration d'une méthode de révision accompagnée d'un facteur temps. Si l'entreprise surveille l'évolution des matériels et des technologies qu'elle met en œuvre, le suivi du processus de mise à jour de la politique de sécurité en sera grandement facilité. Toutefois, les menaces et les techniques de protection en perpétuelle évolution commandent de temps à autre une évolution de la politique de sécurité avant la date de révision planifiée. Ceci doit malgré tout rester exceptionnel car la politique de sécurité de par son mode d'élaboration balaye un large panel de mesures.

4. Agir (Act...)

Lorsque le besoin s'en fait sentir ou lorsque la date planifiée de révision approche, il s'agit après analyse et reflexion de modifier la politique de sécurité dans le but de l'adapter aux menaces qui pèsent sur les services qu'elle couvre ou sur de nouveaux services.

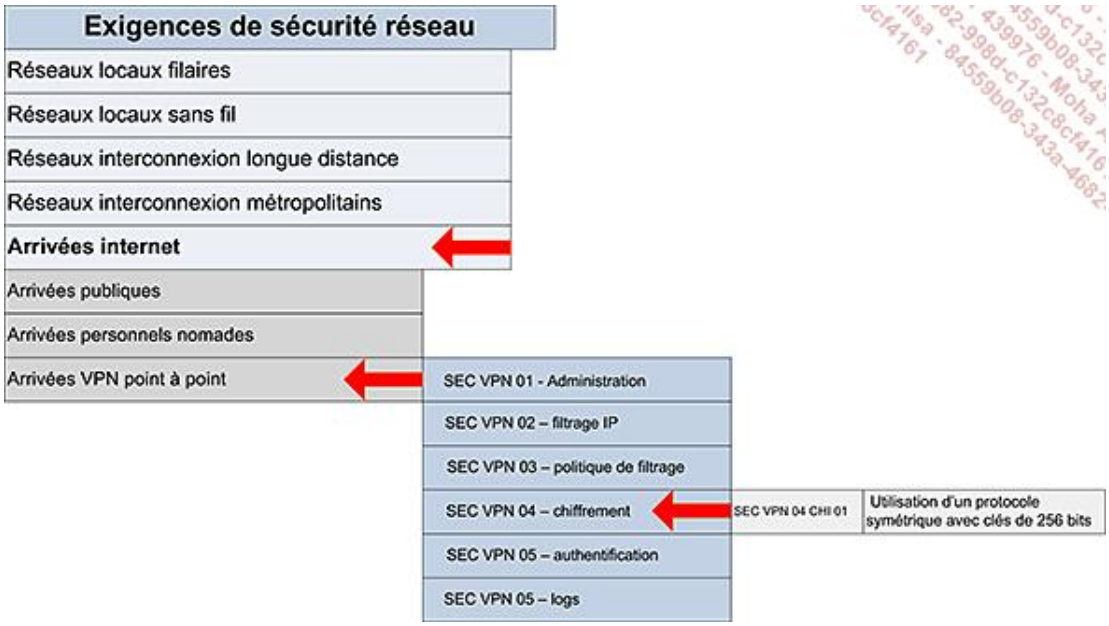
© ENI Editions - All rigths reserved - Moha Anisa

Prenons par exemple le cas des VPN SSL que nous aborderons lors du chapitre consacré aux pare-feu. Cette technique à part entière mérite de se voir consacrer un chapitre de la politique de sécurité car elle met en œuvre des fonctionnalités réparties sur de trop nombreux chapitres pour être exploitable en l'état. Sur ce point, il semble raisonnable d'anticiper l'évolution de la politique de sécurité pour ne pas avoir à gérer en même temps les questions inhérentes à un projet en cours avec celles qui ne manquent pas de se poser lors d'une refonte d'un tel document. L'équipe en charge du suivi de la politique de sécurité passe donc la main à celle en charge de son évolution et de sa révision. Une fois ce processus terminé, la politique de sécurité révisée est remise en service puis diffusée.

© ENI Editions - All rigths reserved - Moha Anisa

Mise en application

Nous allons dans ce livre mettre en pratique la phase de planification du cycle de vie d'une politique de sécurité au travers de chapitres qui au départ suivront les couches qualifiées de basses du modèle OSI. En la matière, le raisonnement en couche est parfaitement adapté car il permet un découpage et un enchaînement logique des tâches qui conduisent à un modèle de sécurité acceptable et applicable. Au-dessus de la couche réseau et de la couche transport nous pénétrons dans l'univers des applications pour lesquelles nous disposons également de fonctions de sécurité avancées.


Exigences de sécurité réseau
Réseaux locaux filaires
Réseaux locaux sans fil
Réseaux interconnexion longue distance
Réseaux interconnexion métropolitains
Arrivées internet
Arrivées publiques
Arrivées personnels nomades
Arrivées VPN point à point
SEC VPN 01 - Administration
SEC VPN 02 – filtrage IP
SEC VPN 03 – politique de filtrage
SEC VPN 04 – chiffrement
SEC VPN 04 CHI 01
Utilisation d'un protocole symétrique avec clés de 256 bits
SEC VPN 05 – authentification
SEC VPN 05 – logs

Pour chacune de ces étapes nous poserons, préalablement à tout développement, une liste d'exigences de sécurité au regard de laquelle nous trouverons les solutions correspondantes. Cette approche, dès les prémices d'un projet a pour avantage de faciliter l'expression ordonnée des besoins ou la rédaction d'un appel d'offre cohérent. En règle générale, les exigences sont classées par grands thèmes génériques qui sont déclinés par la suite en exigences unitaires elles-mêmes accompagnées d'une brève description et parfois de références à d'autres exigences. Cette classification est un fondement de la politique de sécurité. Le schéma représente une vue éclatée d'un extrait des exigences de sécurité réseau. Chaque flèche développe un sous-domaine jusqu'à dévoiler l'exigence qui stipule l'utilisation d'un protocole de chiffrement. Il est à noter qu'aucun produit (aucune marque) n'est ici cité.

Les exigences de sécurité ont pour objectif dans les chapitres qui suivent l'introduction des solutions techniques qui sont proposées par Cisco. À ce titre, elles restent positionnées à un niveau élevé que l'on pourrait qualifier de général, chacun étant libre par la suite de les décliner en fonction de ses propres contraintes.

© ENI Editions - All rigths reserved - Moha Anisa

Conclusion

La politique de sécurité est un élément indispensable et préalable à toute entreprise (dans le sens du mot projet). Elle s'élabore à partir d'une réflexion portant sur la protection des ressources et le niveau d'accès des utilisateurs qui est lui-même fonction d'un niveau de confiance et de responsabilité. Ce document est le fruit d'un travail itératif et doit suivre, voire être en avance, sur l'évolution de l'architecture.

La politique de sécurité est mise à disposition des entités qui travaillent notamment à la planification ainsi qu'à la réalisation de projets. Ces dernières doivent impérativement saisir la nécessité de l'intégrer dès les premières phases en dérivant ses préconisations sous la forme d'exigences destinées à faciliter la rédaction d'appels d'offre ou l'élaboration de l'architecture choisie.

© ENI Editions - All rigths reserved - Moha Anisa

Introduction

Ce chapitre aborde des notions générales et fondamentales sur la protection des réseaux de données et sur les couches dites basses du modèle OSI. Les couches sont interdépendantes logiquement par leurs interfaces communes respectives.

La compromission d'une couche entraîne un risque élevé de compromission des couches supérieures

Les notions que nous allons aborder concernent la couche physique et sont applicables quel que soit le fabricant du matériel utilisé. L'objectif de ce chapitre est de décrire et de classifier les menaces les plus courantes pour s'en protéger grâce aux possibilités offertes par les équipements du réseau.

© ENI Editions - All rigths reserved - Moha Anisa

Sécurité et couche physique

La couche physique permet la transmission du signal électrique ou optique émis par les interfaces réseau. Cette transmission s'effectue sur un câble à paires torsadées, sur fibre optique ou par radio. Les méthodes de codage de l'information et les caractéristiques techniques de chaque média sont choisies en fonction de l'architecture désirée.

Dès les premières ébauches d'une nouvelle architecture réseau ou au cours d'une migration, la sécurité autour de la couche physique doit être considérée avec attention car, tout comme la qualité de transmission de l'information résulte de la qualité de la couche physique, la sécurité de l'information découle aussi du niveau de protection de cette couche. Les exemples, hélas, se comptent par dizaines. Les écoutes, les interceptions, hormis le vol direct de l'information à la source, sont trop souvent la conséquence d'une mauvaise protection de la couche physique.

Toutefois, les mesures de protection, toujours indépendantes du choix d'un constructeur, sont relativement simples à mettre en œuvre. Nous citerons entre autres la protection des locaux dans lesquels résident les équipements d'interconnexion et la sélection de médias appropriés. Enfin une attention toute particulière sera portée sur l'accès au réseau.

© ENI Editions - All rigths reserved - Moha Anisa

La protection des accès au réseau

Les types d'accès au réseau sont par nature dépendant du média utilisé. Quel que soit ce dernier (fibre, câble, radio) il est primordial d'en limiter strictement l'accès aux personnels dûment autorisés. En la matière, les audits et autres tests de pénétration (et bien entendu les personnes mal intentionnées) débutent en règle générale leur travail (ou leurs agissements) en s'efforçant de connecter leurs équipements sur le réseau ciblé par tous les moyens s'offrant à eux sans effraction notable. Citons, sans rechercher une quelconque exhaustivité, les petits concentrateurs utilisés pour prolonger le réseau dans certains bureaux, les points d'accès sans fil déployés sans en référer aux responsables de l'infrastructure ou encore, les connecteurs muraux derrière lesquels on peut espérer trouver un signal.

1. Le cas du connecteur mural

Il s'agit de l'accès le plus largement disponible. Il fut introduit avec l'avènement des ordinateurs individuels connectés en réseau au début des années 90.

L'accès au réseau par connecteur mural de type RJ45 (Ethernet) est toujours largement répandu. La carte réseau de l'ordinateur est reliée par un cordon à une prise murale. De cette prise part (dans le sol, le faux plafond, ou le mur) un câble en cuivre à paires torsadées qui aboutit sur un panneau de raccordement. Ce panneau (baie de brassage) regroupe les arrivées qui correspondent aux bureaux d'un ou plusieurs étages. Enfin, les connecteurs de ce panneau sont reliés nombre pour nombre aux ports de l'équipement réseau dont la configuration nous intéresse.

2. Le cas du point d'accès sans fil (Access Point Wi-Fi)

Les accès aux réseaux sans fil se sont considérablement démocratisés depuis les années 2000. L'intérêt principal réside dans la possibilité pour un utilisateur de se déplacer librement tout en restant connecté au réseau. Ainsi depuis quelques années, les accès sans fil s'offrent à tout un chacun dans divers lieux publics afin d'accéder au réseau Internet.

Au sein des réseaux d'entreprise, la technologie Wi-Fi offre la possibilité avec une infrastructure unique de se connecter à tout le réseau local pour les personnels autorisés ou uniquement à Internet pour les personnes extérieures.

L'infrastructure sans fil se compose principalement de points d'accès alliant la technologie radio à celle plus classique de l'Ethernet sur câble. Cette dernière connexion relie le point d'accès au réseau traditionnel. Dès l'introduction de la technologie Wi-Fi, les points d'accès au réseau ont embarqué des fonctions de sécurité visant à protéger les informations et les accès. La cryptographie est largement utilisée pour y parvenir.

3. Les premières mesures de protection

Sans pour l'instant aborder la configuration proprement dite d'un équipement (mais nous y viendrons) quelques mesures s'imposent d'elles-mêmes pour contribuer à l'amélioration de la sécurité du réseau.

Nous avons brièvement décrit les moyens principaux qui donnent accès au réseau. Certaines précautions empêchent physiquement les connexions et parmi celles-ci, la plus simple à mettre en œuvre consiste à introduire une coupure sur le lien. Dans le cas d'un réseau câblé, il suffit simplement de ne pas connecter la prise murale à l'équipement réseau. Cette méthode fort simple n'est que rarement utilisée et nombreux sont les réseaux accessibles à partir d'une prise murale à partir des endroits les plus anodins. Une autre méthode consiste sur l'équipement réseau à fermer administrativement les ports qui ne sont pas reliés à un ordinateur. Tout ceci requiert une bonne organisation. Dans un cas comme dans l'autre, les opérateurs du réseau câblent ou retirent le câblage à la demande en fonction des mouvements internes des employés. De même, ils procèdent à l'activation ou à la désactivation des ports sur l'équipement de raccordement.

Les accès sans fil sont par nature plus difficiles à protéger contre les tentatives physiques de connexion par le réseau radio. Ils sont vulnérables à des attaques sur les ports câblés qui sont, rappelons-le, quasi directement connectés au reste du réseau. Les ondes radios quant à elles ne connaissent pas les frontières. Une approche de protection consiste à positionner les points d'accès sans fil au plus loin des zones publiques. Le port Ethernet étant pour sa part habillement protégé afin d'interdire tout accès physique. Cette protection s'apparente à celle d'un distributeur de billets de banque où l'écran est visible du côté accessible au public (les antennes dans le cas du point d'accès) alors que la réserve de billets (le port Ethernet) est hors d'atteinte.

Chaque entreprise dans son plan de sécurité est encouragée à isoler les zones publiques des zones privées faisant partie du réseau dit interne. Les zones publiques mettent à disposition des visiteurs un accès à Internet faiblement contrôlé grâce à une borne Wi-Fi au rayonnement réduit. Le passage d'une zone à l'autre nécessite une authentification. Malgré tout, les accès à Internet de type « invités » (filaire ou Wi-Fi) peuvent rester disponibles dans des zones telles que les salles de réunions dans lesquelles des personnes étrangères à l'entreprise sont autorisées à pénétrer. Dans ce dernier cas, une isolation logique ou physique sera mise en œuvre afin de garantir la séparation

© ENI Editions - All rigths reserved - Moha Anisa

entre le réseau « invités » et le réseau de production.

Pour conclure, citons le cas des locaux dans lesquels se trouvent les équipements réseau. Il va de soi que leur protection requiert une attention toute particulière. Dans ce domaine, il est fortement recommandé de faire appel à un professionnel de la sécurité physique maîtrisant les techniques de contrôle d'accès, de blindage, et de protection contre les rayonnements électromagnétiques.

© ENI Editions - All rigths reserved - Moha Anisa

Sécurité et couche liaison de données

Nous abordons à présent la partie pour laquelle nous allons décrire puis mettre en œuvre matériellement les possibilités qui nous sont offertes par les équipements Cisco.

C'est à partir de la couche liaison de données qu'apparaît la notion d'adresse réseau. Cette couche est responsable de la communication d'entités par le biais d'un média commun. Ses fonctions comprennent entre autres la génération des trames et la détection d'erreurs. Parmi les protocoles de niveau deux les plus connus nous trouvons Ethernet et PPP.

Comme nous l'avons décrit lors du chapitre précédent, une politique de sécurité est indispensable pour assurer un développement et un suivi cohérent de la protection des données. Cette politique couvre les aspects afférents au réseau de l'entreprise. Il en va de même lors d'un projet réseau dont un volet abordera et prendra en compte la sécurité. Afin de sélectionner dans le cadre d'un appel d'offre plusieurs candidats, l'élaboration d'un cahier des charges précis s'avère indispensable. C'est sur ce point qu'intervient l'équipe ou le responsable chargé de la sécurité. Il doit fournir ses exigences qui transcrites dans le cahier des charges, sont fournies aux équipementiers. Pour chaque exigence, un degré de priorité est précisé. Enfin, en regard de chaque exigence, l'équipementier renseigne une case avec ses commentaires. Voici un exemple dans le tableau suivant que nous avons volontairement simplifié, libre à vous de l'étendre en fonction de vos exigences.

Exigences de sécurité de l'équipement réseau pour la couche 2		
Exigences	**Degrés de priorité**	**Réponses**
Limiter l'accès au port à une liste d'adresses Mac.	Obligatoire	Disponible sur les modèles…
Création de VLAN.	Obligatoire	Disponible au-delà du modèle…
Implémentation de la norme 802.1X.	Souhaité	Indisponible avant 2 ans.
Création de VLAN privés.	Optionnel	Indisponible

Cette présentation s'étendra éventuellement à toutes les fonctionnalités de l'équipement. C'est de ce type de tableau que découle le cahier de test et d'évaluation du matériel dans lequel les exigences obligatoires figureront avec le résultat du test visant à en vérifier le bon fonctionnement.

1. Exigences et risques de sécurité pour la couche liaison de données

Posons tout d'abord nos exigences de sécurité sous la forme d'un tableau et mettons-les en regard des solutions techniques que CISCO nous apporte. Nous partons du principe que toutes les exigences revêtent un caractère obligatoire.

Exigences de sécurité de l'équipement réseau pour la couche 2	
Exigences	**Technique**
Limiter les adresses Mac par port.	port security
Authentifier l'accès au réseau.	802.1x
Limiter les échanges dans un VLAN.	private VLAN
Interdire le changement de VLAN.	Configuration
Préserver l'intégrité d'une communication.	Sticky arp, dynamic arp inspection,
Protéger les attaques dans les VLAN.	dynamic arp inspection
Empêcher l'installation de serveurs DHCP non autorisés.	DHCP Snooping

© ENI Editions - All rigths reserved - Moha Anisa

Nous pouvons extrapoler de ce tableau les attaques dirigées vers la couche 2. Ce sont (dans l'ordre du tableau) :

- les attaques par « mac flooding » ;
- le changement de VLAN ou « VLAN hopping » ;
- les attaques « Man In The Middle » ;
- les attaques au sein d'un VLAN ;
- les interruptions de services (parfois involontaires) par introduction d'un serveur DHCP non officiel.

2. Descriptions des attaques et prévention

Nous allons nous attacher pour chaque type d'attaque à donner un exemple qui corresponde à la réalité d'un réseau de production en y associant les risques potentiels. Notons que cette notion de risque peut servir de base à la définition des exigences de sécurité.

a. Les attaques par mac flooding

Un commutateur Ethernet est communément désigné par l'appellation de switch. Si un concentrateur Ethernet ou hub est un équipement sans intelligence (parfois comparé à une multiprise) le switch quant à lui possède une table CAM (*Content Addressable Memory*) dans laquelle sont inscrits des couples port - adresse MAC. Les ponts possédaient déjà une table de ce type mais en revanche n'avaient qu'un nombre de ports très limités. Voici un aperçu de l'attaque *mac flooding*.

Flooding signifie à peu de choses près inondation. Cette attaque bien connue consiste à saturer la table CAM du switch en lui envoyant plusieurs milliers d'entrées. Le switch, pour les couples qu'il ne connait pas recopie leur trafic sur tous ses ports au lieu de ne l'envoyer qu'aux ports concernés. La description de cette attaque est largement documentée. Toutefois, bien qu'elle soit simple à mener grâce à un petit outil nommé *macof*, le switch sous attaque voit ses performances se dégrader considérablement au point que les ordinateurs connectés ont le plus grand mal à placer leurs trames sur le réseau. Nous avons reproduit cette attaque sur un switch du modèle Cisco 2950. Après avoir saturé la table CAM avec l'aide de l'outil *macof* (et avoir arrêté ce dernier) nous avons réussi à capturer du trafic unicast au sein d'un VLAN, c'est-à-dire le trafic direct entre deux machines. Cette capture est possible si les deux machines ne sont pas connues du switch au moment de la saturation.

```
6b:1e:a1:69:40:47 2e:2d:5:f:5f:c0 0.0.0.0.11073 > 0.0.0.0.51834: S 1129167564:1129167564(0) win 512
4c:fb:b0:5f:f9:e8 14:15:8:36:b1:31 0.0.0.0.52582 > 0.0.0.0.6996: S 31083328:31083328(0) win 512
c4:45:10:7a:1f:c2 b:5b:2c:7c:c7:db 0.0.0.0.30975 > 0.0.0.0.20188: S 553333133:553333133(0) win 512
b8:8c:83:5d:94:5a 56:fc:76:2:70:26 0.0.0.0.57859 > 0.0.0.0.50740: S 1806200342:1806200342(0) win 512
ae:fe:eb:26:bb:b4 39:ff:dd:49:b6:70 0.0.0.0.26367 > 0.0.0.0.13268: S 820154569:820154569(0) win 512
85:3f:bc:73:80:1 7b:f0:be:5:79:a 0.0.0.0.1224 > 0.0.0.0.54855: S 1845177593:1845177593(0) win 512
cb:a4:9:69:31:5 e5:b:ff:25:a2:c 0.0.0.0.39909 > 0.0.0.0.36260: S 2118227148:2118227148(0) win 512
63:6f:5e:7e:a7:b8 32:59:2e:51:d8:b6 0.0.0.0.23856 > 0.0.0.0.4190: S 608215137:608215137(0) win 512
f5:7c:82:47:e2:f7 b0:50:ac:4f:b1:ba 0.0.0.0.1739 > 0.0.0.0.1828: S 329728069:329728069(0) win 512
c4:c0:af:1d:c2:61 6c:91:83:15:58:10 0.0.0.0.56623 > 0.0.0.0.2634: S 1192696093:1192696093(0) win 512
bb:f7:32:8:f5:cd c7:e7:1d:41:4e:aa 0.0.0.0.15132 > 0.0.0.0.57854: S 1730444157:1730444157(0) win 512
99:5a:42:26:19:27 c5:74:dc:2:38:21 0.0.0.0.40668 > 0.0.0.0.26774: S 219083795:219083795(0) win 512
5e:e8:f6:21:95:df c3:69:c7:6a:45:b1 0.0.0.0.33749 > 0.0.0.0.19742: S 1431762914:1431762914(0) win 512
4f:95:c:28:27:4d 6e:20:92:11:41:e6 0.0.0.0.14469 > 0.0.0.0.45714: S 550303746:550303746(0) win 512
e7:c9:69:68:aa:99 a:80:35:42:f3:a9 0.0.0.0.41969 > 0.0.0.0.22974: S 370144913:370144913(0) win 512
3:c7:83:5:f7:16 d4:d6:d5:2d:12:a1 0.0.0.0.25601 > 0.0.0.0.19474: S 677353815:677353815(0) win 512
79:6f:a3:40:12:7f 3c:8:25:76:1d:e2 0.0.0.0.6381 > 0.0.0.0.7641: S 714767824:714767824(0) win 512
70:3f:8f:79:bb:5a 10:f2:55:59:3f:fb 0.0.0.0.8011 > 0.0.0.0.10401: S 767636037:767636037(0) win 512
4b:d6:69:77:8e:2c ea:7a:f9:47:5e:d2 0.0.0.0.18167 > 0.0.0.0.45473: S 738306864:738306864(0) win 512
6c:63:6f:7f:4f:87 72:cd:4e:3a:3c:e1 0.0.0.0.55060 > 0.0.0.0.33369: S 1508258056:1508258056(0) win 512
7b:f1:9a:42:ed:c3 f7:79:43:60:7b:ff 0.0.0.0.1477 > 0.0.0.0.56952: S 1390458026:1390458026(0) win 512
56:71:f:19:3f:d5 e:ff:4a:13:49:4d 0.0.0.0.55400 > 0.0.0.0.28310: S 498037739:498037739(0) win 512
54:dc:ef:1a:75:f4
```

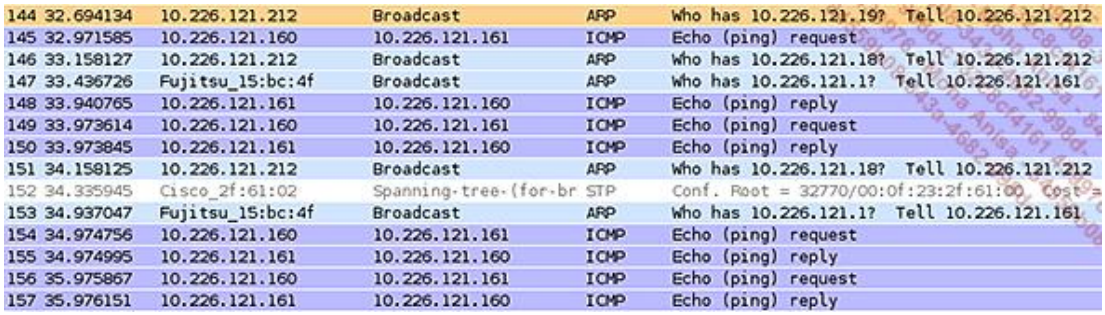
Voici une capture d'écran montrant *macof* envoyant des trames dont l'adresse MAC est générée aléatoirement.

```
Switch# sh mac-address-table count

Mac Entries for Vlan 2:
---------------------------
Dynamic Address Count  : 5088
Static  Address Count  : 0
Total Mac Addresses    : 5088
```


© ENI Editions - All rigths reserved - Moha Anisa

```
Total Mac Address Space Available: 0
```

Au bout de quelques secondes, la table CAM du switch est saturée comme l'indique ici le total des adresses MAC disponible.



144	32.694134	10.226.121.212	Broadcast	ARP	Who has 10.226.121.19? Tell 10.226.121.212
145	32.971585	10.226.121.160	10.226.121.161	ICMP	Echo (ping) request
146	33.158127	10.226.121.212	Broadcast	ARP	Who has 10.226.121.18? Tell 10.226.121.212
147	33.436726	Fujitsu_15:bc:4f	Broadcast	ARP	Who has 10.226.121.1? Tell 10.226.121.161
148	33.940765	10.226.121.161	10.226.121.160	ICMP	Echo (ping) reply
149	33.973614	10.226.121.160	10.226.121.161	ICMP	Echo (ping) request
150	33.973845	10.226.121.161	10.226.121.160	ICMP	Echo (ping) reply
151	34.158125	10.226.121.212	Broadcast	ARP	Who has 10.226.121.18? Tell 10.226.121.212
152	34.335945	Cisco_2f:61:02	Spanning-tree-(for-br	STP	Conf. Root = 32770/00:0f:23:2f:61:00 Cost =
153	34.937047	Fujitsu_15:bc:4f	Broadcast	ARP	Who has 10.226.121.1? Tell 10.226.121.161
154	34.974756	10.226.121.160	10.226.121.161	ICMP	Echo (ping) request
155	34.974995	10.226.121.161	10.226.121.160	ICMP	Echo (ping) reply
156	35.975867	10.226.121.160	10.226.121.161	ICMP	Echo (ping) request
157	35.976151	10.226.121.161	10.226.121.160	ICMP	Echo (ping) reply

Le switch diffuse sur tous les ports le trafic (un ping) entre deux stations dont il découvre les adresses MAC ne sachant pas où elles sont physiquement localisées.

La commande port-security

Afin de contrer une telle attaque, Cisco propose une commande `switchport port-security` dont les options permettent :

- de limiter le nombre d'adresses MAC associées à un port du switch ;
- de réagir en cas de dépassement de ce nombre ;
- de fixer une adresse MAC sur un port ;
- de ne retenir que la première adresse MAC qui se présente.

Configuration et vérification

Décrivons les quatre étapes nécessaires à la configuration de ces fonctions :

- La fonction `port-security` est dans un premier temps activée globalement au niveau de l'interface :

```
SW0(config)#int fastEthernet 0/2
SW0(config-if)#switchport port-security
```

- Puis, il faut renseigner le mode d'apprentissage des adresses MAC qui seront associées au port. À ce stade, l'adresse est entrée manuellement ou bien apprise par le switch par le biais de l'option `sticky`.

```
SW0(config-if)#switchport port-sec mac-address 0018.8B
7E.20E9
```

ou,

```
SW0(config-if)# switchport port-security mac-address sticky
```

- Il faut par la suite indiquer au switch le nombre maximal d'adresses qu'il tolèrera sur le port (2 dans la commande ci-dessous).

```
SW0(config-if)#switchport port-security maximum 2
```

- Il faut finalement indiquer au switch la façon dont il réagira en cas de dépassement du nombre d'adresses MAC autorisé. Trois modes sont disponibles :

© ENI Editions - All rigths reserved - Moha Anisa

- rejet des adresses en dépassement sans notification, mode `protect` ;
- rejet des adresses en dépassement avec notification, mode `restrict` ;
- fermeture du port, mode `shutdown` (mode par défaut).

```
SW0(config-if)#switchport port-security violation shutdown
```

Voici, quelques configurations complètes d'une interface :

```
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security violation restrict
 spanning-tree portfast
```

```
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address 0018.abcd.abcd
 switchport port-security violation restrict
 spanning-tree portfast
```

Dans cette dernière configuration, sur la 6ème ligne, nous observons l'adresse MAC apprise dynamiquement grâce à l'utilisation de la commande `sticky`.

Vérifions le comportement du switch lors d'une attaque par saturation de la table CAM. Le switch est configuré pour fermer le port en cas de dépassement de la valeur autorisée.

```
*Mar  1 01:15:36 CET: %PM-4-ERR_DISABLE: psecure-violation error
detected on Fa0/2, putting Fa0/2 in err-disable state
SW0#
*Mar  1 01:15:36 CET: %PORT_SECURITY-2-PSECURE_VIOLATION: Security
violation occurred, caused by MAC address 66a7.644e.3976 on port
FastEthernet0/2.
SW0#
*Mar  1 01:15:37 CET: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/2, changed state to down
SW0#
*Mar  1 01:15:38 CET: %LINK-3-UPDOWN: Interface FastEthernet0/2,
changed state to down
```

L'interface est belle et bien fermée. Pour la remettre en service nous utilisons la séquence suivante :

```
SW0(config-if)#shut down
SW0(config-if)#no shut down
```

Dans le cas d'un téléphone IP sur lequel se trouve connecté un PC, trois adresses MAC sont nécessaires au bon fonctionnement de l'ensemble. La commande sera donc `switchport port-security maximum 3`.

Une adresse MAC apprise et inscrite dans la configuration courante (option `sticky`) n'est pas sauvegardée en cas d'extinction du switch.

Respecter la séquence `shut` puis `no shut` afin de remettre en service l'interface.

La commande `shutdown` permet de fermer "administrativement" un port. Cela équivaut en quelque sorte à une déconnexion virtuelle du câble réseau car ce dernier reste physiquement connecté. La commande `no`

© ENI Editions - All rigths reserved - Moha Anisa

shutdown permet d'ouvrir le port.

Comme toujours, les commandes show permettent de vérifier le résultat du paramétrage.

Les commandes chez Cisco possèdent pour la plupart d'entre elles une forme abrégée. La commande show se résume par le condensé sh.

```
SW0#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation
Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------
-
     Fa0/2          3            1                 0
Protect
---------------------------------------------------------------------
-
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

b. Les accès illicites au réseau et le protocole 802.1X

La sécurité d'un réseau débute à sa porte d'entrée. Nous avons décrit une méthode simple afin d'empêcher une connexion au réseau qui consiste à déconnecter le câblage d'infrastructure. Cette façon de procéder est toutefois très contraignante. Heureusement les switchs (et les routeurs) Cisco possèdent une commande qui permet à l'administrateur de fermer à distance un port d'accès. Il s'agit de la commande shutdown. Cette pratique n'est pas adaptée pour un réseau comprenant plusieurs centaines ou plusieurs milliers d'utilisateurs. Une autre méthode est nécessaire pour décharger les équipes d'administration d'une tâche si répétitive.

Description et fonctionnement

802.1x est un standard qui définit un mécanisme d'authentification pour l'accès au réseau. 802.1x peut être comparé au protocole PPP largement diffusé à l'époque (pas si lointaine) où l'accès à Internet nécessitait l'utilisation d'un modem. Le protocole PPP s'appuyait sur un mécanisme embarqué chargé de l'authentification pour lequel deux sous-protocoles étaient proposés au choix : PAP et CHAP. Schématiquement, nous pourrions écrire : accès Internet = modem + PPP + (PAP ou CHAP) + TCP/IP.

802.1X s'il est utilisé sur un équipement tel qu'un switch oblige l'utilisateur connectant son ordinateur au réseau (filaire ou sans fil) à s'authentifier avant d'entamer toute activité. À l'issue du processus d'authentification (et en cas de succès) le client reçoit un profil réseau (TCP/IP et VLAN) ainsi qu'un assortiment de règles de sécurité.

802.1X s'appuie sur EAP (*Extensible Authentication Protocol*). EAP est un moyen de transporter un protocole d'authentification. C'est pourquoi il existe autant d'appellations autour d'EAP que de protocoles d'authentification embarqués. EAP transporté sur un lien Ethernet est dénommé EAPOL pour *EAP Over Lan*. Citons à titre d'exemple :

- LEAP (protocole propriétaire Cisco) ;
- EAP-MD5 (qui transporte des messages « hachés » par MD5) ;
- EAP-TLS (authentification basée sur l'échange de certificats) ;
- PEAP (qui transporte une authentification Microsoft CHAP Version 2) ;
- EAP-FAST (proposé par CISCO pour remplacer LEAP).

Nous allons détailler le fonctionnement de 802.1X avec l'utilisation de PEAP dans le cadre d'une connexion Ethernet. PEAP est proposé sur les systèmes d'exploitation Microsoft XP et Vista.

802.1X fait intervenir 3 entités :

- le **client** (ou supplicant en terminologie anglaise) est typiquement un PC ;
- le **switch** (ou authenticator) ;

© ENI Editions - All rigths reserved - Moha Anisa

- le **serveur** d'authentification (ou authentication server) qui est un serveur RADIUS.

Les messages EAP transportent les échanges d'authentification entre le client et le serveur d'authentification. Le switch ne fait que les relayer, toutefois de part et d'autre du switch, les messages EAP ne sont pas transportés de la même façon.

- Entre le client et le switch, EAP est directement dans la charge utile des trames Ethernet.
- Entre le switch et le serveur RADIUS, EAP est transporté dans les messages RADIUS.

Les échanges EAP entre le client et le serveur RADIUS passent par deux phases :

- Une série d'échanges comportant l'identité du client et les paramètres de mise en place d'un tunnel TLS.
- L'établissement du tunnel TLS dans lequel transitera le protocole d'authentification MSCHAP V2.

À l'issue de ces échanges et si l'authentification est correcte, le serveur RADIUS ordonne au switch de connecter pleinement le client au réseau. Pour terminer, le client et le switch reçoivent éventuellement des paramètres en provenance du serveur RADIUS comme un numéro de VLAN, une adresse IP ou encore une liste de filtrage ACL (*Access Control List*).

Si l'authentification n'aboutit pas, le client voit sa demande de connexion rejetée. Il est éventuellement dirigé vers un VLAN d'attente à la connectivité limitée. Tant que le client n'est pas authentifié, seules les trames EAP transitent entre le client et le switch à l'exclusion de tout autre protocole supérieur tel que TCP/IP.

Variante de déploiement

Nous utiliserons un client 802.1X et l'implémentation du protocole RADIUS fournis par Microsoft. Ce service RADIUS est également disponible avec un serveur ACS de chez Cisco ou sur un serveur Linux (FreeRADIUS). De nombreuses implémentations de RADIUS sont disponibles par ailleurs.

Nous ne décrirons pas dans le détail l'installation des composants de la partie Microsoft. Nous présenterons une liste des fonctions à activer. L'installation d'un serveur RADIUS afin d'authentifier des utilisateurs avec 802.1X requiert :

- une installation fonctionnelle de Microsoft Windows 2000 ou 2003 Server en tant que contrôleur de domaine Active Directory (y compris les services DNS) ;
- la création des utilisateurs avec autorisation d'accès distant ;
- le regroupement des utilisateurs dans des groupes globaux qui seront utilisés par les politiques d'accès ;
- le service de certificats en ayant pris soin de générer un certificat auto signé pour le serveur ;
- le service d'authentification Internet qui sera enregistré dans l'Active Directory.
    - Le switch fournissant le service 802.1X sera déclaré en tant que client.
    - Une ou plusieurs politiques d'accès en fonction :
        - des adresses IP des points d'accès (NAS)
        - du groupe d'utilisateur à authentifier
        - des attributs RADIUS définissant le VLAN dans lequel diriger l'utilisateur une fois authentifié :
            - Tunnel-Type[64]=VLAN
            - Tunnel-Medium-Type[65]=802
            - Tunnel-Private-Group-Id[81]=*Nom du VLAN*

© ENI Editions - All rigths reserved - Moha Anisa

- Le certificat précédemment émis sera déclaré dans les propriétés EAP (propriétés d'authentification du profil de la politique).

- Sur les postes de travail :

  - activation de l'authentification dans les propriétés de la connexion réseau (pour Vista dépend du service Configuration automatique de réseau câblé qui est désactivé par défaut) ;

  - paramétrage de PEAP (en choisissant ou non de vérifier le certificat du serveur RADIUS).

Voici à présent la configuration du switch 2950 :

```
SW0#sh run
Building configuration...
!
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

dot1x system-auth-control
dot1x guest-vlan supplicant
!
!
interface FastEthernet0/11
 switchport mode access
 switchport port-security maximum 3
 dot1x port-control auto
 spanning-tree portfast
!
radius-server host 10.xxx.xxx.42 key 7 030752180500
```

Décrivons cette configuration :

- La commande `aaa new-model` active les fonctions d'authentification, d'autorisation et de comptabilité du switch. Les trois commandes suivantes définissent les services du serveur RADIUS (déclaré plus bas) qui aura la charge d'authentifier les utilisateurs, de leur affecter éventuellement un VLAN d'accueil et de garder une trace de leur durée de connexion.

- La commande globale `dot1x system-auth-control` active 802.1X pour tout le switch.

- La commande globale `dot1x guest-vlan supplicant` dirige les clients qui ne supportent pas 802.1X ou dont l'authentification a échoué vers un VLAN prévu à cet effet.

- La commande (en mode interface) `dot1x port-control auto` active 802.1x sur l'interface et demande au port de suivre les instructions du protocole lui ordonnant de s'ouvrir (en cas de succès) ou de ne pas donner accès au réseau.

- La commande `radius-server` déclare le serveur RADIUS qui fournit les services demandés ainsi qu'une clé d'authentification.

c. Sécurité et VLANs

Sur un switch, un VLAN est un groupe de ports. Les machines connectées à ces ports peuvent communiquer entre elles librement. En revanche, toute communication est impossible avec un port étranger au VLAN. On imagine aisément deux réseaux câblés isolés l'un de l'autre et qui de fait ne communiquent pas. Répartis sur un réseau Ethernet commuté, les VLAN offrent par exemple une solution pratique pour isoler les unes des autres des sociétés partageant une infrastructure commune. Après avoir été largement promue et recommandée, cette technique est maintenant remplacée par le déploiement de réseaux routés au plus près de l'utilisateur final. Toutefois, les VLAN n'ont pas totalement disparus. On les rencontre toujours sur les équipements d'extrémité, là où les utilisateurs (ou les serveurs) sont physiquement connectés.

De nouvelles exigences de sécurité découlent de l'utilisation des VLAN. En effet, il est indispensable de garantir que

© ENI Editions - All rigths reserved - Moha Anisa

deux populations censées être isolées l'une de l'autre le sont effectivement.

Sécurité à l'intérieur d'un VLAN (VLAN ACL, Private VLAN, Dynamic Arp inspection)

Les attaques virales qui ont ébranlé les réseaux d'entreprises ces dernières années ont prouvé la nécessité de posséder un niveau d'isolation supplémentaire au sein des VLAN. Les vers ayant causé le plus de dégâts embarquaient un dispositif permettant l'expansion rapide de l'attaque aux machines les plus proches. Ainsi, les réseaux directement connectés une fois connus par le vers, furent inondés de messages jusqu'à l'effondrement.

À l'intérieur d'un VLAN d'utilisateurs, la politique de sécurité impose parfois une isolation des postes de travail entre eux afin qu'aucune donnée ne soit partagée directement. Une exigence identique est envisageable dans un VLAN où se trouvent des serveurs.

Les communications directes entre les membres d'un même VLAN si elles sont autorisées doivent toutefois être protégées contre toute tentative d'intrusion visant à l'usurpation d'identité ou de données, c'est pourquoi des contrôles avancés sur la couche liaison de données viennent renforcer ceux que nous avons précédemment décrits.

Les VLAN ACL

Les VLAN ACL (pour *VLAN Access Control Lists*) s'apparentent aux ACL de niveau trois c'est-à-dire aux ACL qui s'appliquent sur les interfaces routées. Mais comme leur nom l'indique, elles s'apposent dans des VLAN ou plus exactement à tous les paquets qui y entrent. Il est ainsi possible de limiter le trafic au sein même d'un VLAN.

Les VLAN ACL (ou VACL) sont définies dans la configuration par une suite de séquences numérotées. Chaque séquence comprend une identification du trafic à traiter et une action à lui administrer, le tout est ensuite appliqué au VLAN à protéger.

Parmi les actions figure au côté des options `drop` et `forward` l'option `capture`. Elle permet de capturer le trafic et de le copier vers un port sur lequel une sonde de détection d'intrusion est connectée.

Les étapes pour la mise en œuvre des VACL sont :

- La programmation d'une ou plusieurs ACL classiques qui sont examinées l'une après l'autre en séquence. Ces ACL sont basées sur des adresses IP ou MAC.
- La création de la VACL qui appelle l'ACL précédemment définie et décide d'une action.
- L'application de la VACL au VLAN dans lequel on souhaite filtrer le trafic.

Les écrans qui suivent montrent un cas simple permettant aux stations d'un VLAN de sortir vers Internet (via un proxy) en ayant au préalable interrogé un serveur DNS.

```
Switch#conf t
Switch(config)#
Switch(config)#ip access-list extended juste-internet
Switch(config-ext-nacl)#10 permit udp any host DNS1 eq domain
Switch(config-ext-nacl)#15 permit udp any host DNS2 eq domain
Switch(config-ext-nacl)#20 permit udp host DNS1 eq domain any
Switch(config-ext-nacl)#25 permit udp any host DNS2 eq domain
Switch(config-ext-nacl)#30 permit tcp any host PROXY eq 8080
Switch(config-ext-nacl)#35 permit tcp host PROXY eq 8080 any
Switch(config-ext-nacl)#end
Switch#
```

L'abréviation `conf t` condense la commande `configuration Terminal` qui donne accès au mode de configuration de l'équipement via une console ou un terminal.

La commande `end` permet de sortir du mode de configuration (et de tous ces sous-modes) pour revenir directement à l'invite de commande (en anglais "prompt").

L'ACL de type étendue nommée *juste-internet* comporte 6 séquences permettant au trafic issu du VLAN de sortir (et de revenir) pour l'activité DNS (domain) et WEB sur le port TCP 8080. Deux serveurs DNS et un serveur proxy HTTP sont déclarés.

```
Switch#conf t
Switch(config)#vlan access-map limitation 10
Switch(config-access-map)#match ip address juste-internet
```


© ENI Editions - All rigths reserved - Moha Anisa

```
Switch(config-access-map)#action forward
Switch(config-access-map)#end
Switch#
```

Ici, la VACL est créée. Elle se nomme *limitation* et porte le numéro de séquence 10. Elle appelle (pour la séquence 10) l'ACL *juste-internet* précédemment créée et permet au trafic autorisé par l'ACL de quitter le VLAN (action forward).

```
Switch# conf t
Switch(config)# vlan filter limitation vlan-list 2
Switch(config)#^Z
Switch#
```

Pour terminer, la VACL *limitation* est appliquée au VLAN à filtrer, ici le VLAN 2.

```
Switch#sh ip access-lists
Extended IP access list juste-internet
    10 permit udp any host DNS1 eq domain
    15 permit udp any host DNS2 eq domain
    20 permit udp host DNS1 eq domain any
    25 permit udp host DNS2 eq domain any
    30 permit tcp any host PROXY eq 8080
    35 permit tcp host PROXY eq 8080 any
```

```
Switch#sh vlan filter
VLAN Map limitation is filtering VLANs:
  2
```

```
Switch#sh vlan access-map
Vlan access-map "limitation"  10
  Match clauses:
    ip  address: juste-internet
  Action:
    forward
```

Les commandes *show* nous fournissent des informations qui permettent de vérifier la configuration. Les commandes utiles sont `sh ip access-lists`, `sh vlan filter` et `sh vlan access-map`. Cet exemple est relativement simple car il présente une unique séquence tant pour l'ACL que pour l'*access-map*. Il est tout à fait possible de rallonger les séquences pour plus de granularité.

Les Private VLAN

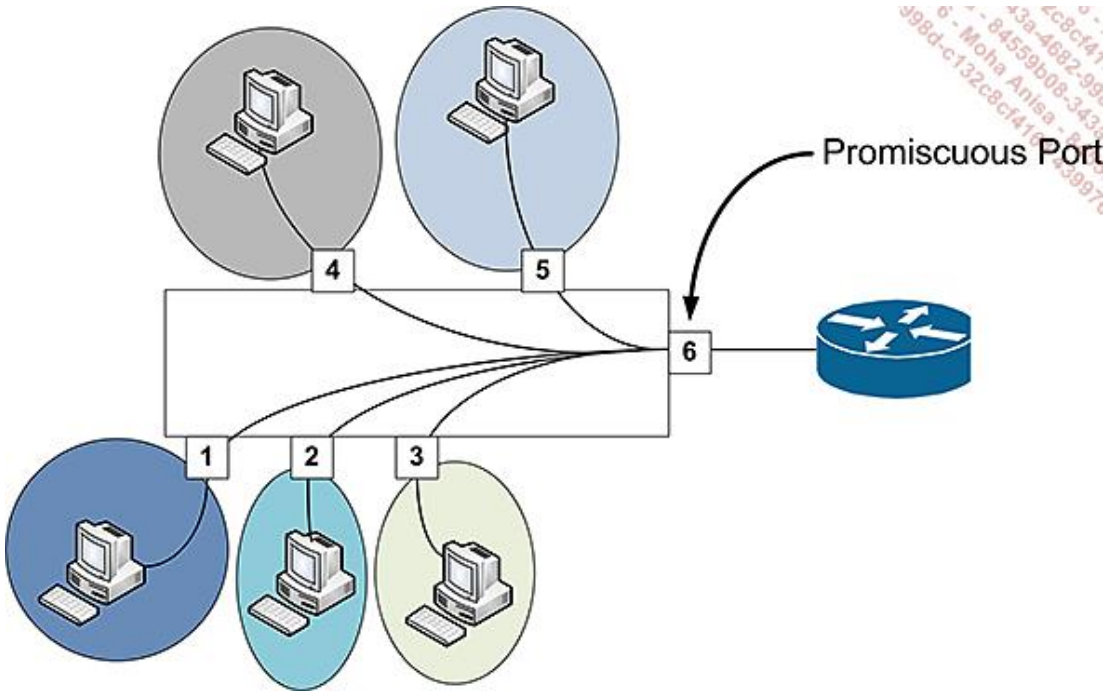
L'objectif des *Private VLAN* est de fournir une isolation au niveau 2 entre des ports connectés au même VLAN. Un exemple typique au sein d'un VLAN est d'interdire aux stations de communiquer entre elles directement et de ne leur laisser que le routeur par défaut comme porte de sortie. Avant cette technique, une solution consistait à créer autant de sous-réseaux IP que de groupes à isoler.

Il est important de se renseigner afin de déterminer si le switch et la version du logiciel IOS vous permettent de déployer cette fonctionnalité. Si elle n'est pas disponible, une commande alternative offre sur certains modèles une fonction équivalente. Les contraintes et limitations à l'emploi des *Private VLAN* sont nombreuses. Nous vous invitons à vous référer à la documentation correspondant à votre modèle de switch et à celle de son système d'exploitation IOS ou CATOS.

Entre autres contraintes :

- Le switch doit être configuré mode VTP transparent.
- Un seul VLAN secondaire de type *isolated* peut être rattaché au VLAN primaire.

© ENI Editions - All rigths reserved - Moha Anisa



Ici, les ports de 1 à 5 ne peuvent communiquer qu'avec le port 6.

Avant d'aborder la configuration, une bonne compréhension de la terminologie s'impose.

La technologie *Private VLAN* fait appel à trois types de VLAN et trois types de ports. On trouve pour les VLAN :

- Le VLAN de type *primary* sur lequel se regroupent les VLAN secondaires.
- Les VLAN secondaires de type :
  - *isolated* (les ports membres sont isolés entre eux) ;
  - *community* (seuls les ports d'une même communauté peuvent communiquer entre eux).

Quant aux ports les trois types sont :

- *promiscuous*. Ce type de port appartient au VLAN primaire et peut communiquer avec tous les autres types de ports des VLAN secondaires associés au VLAN primaire. Il est utilisé pour acheminer le trafic hors du VLAN.
- *isolated*. Ce type de port membre d'un VLAN *isolated* est isolé des autres ports (dans son VLAN) et ne peut communiquer qu'avec le port promiscuous.
- *community*. Ce type de port membre d'un VLAN *community* ne peut communiquer qu'avec les ports de sa communauté et le port promiscuous.

La configuration comprend plusieurs étapes :

- La déclaration des VLAN et de leur type. Cette étape comprend la création d'un VLAN primaire et de tous les VLAN secondaires (*isolated*, *community* ou les deux).
- L'association des VLAN secondaires au VLAN primaire.
- L'association des VLAN secondaires à l'interface de niveau 3 du VLAN *primary* (interface vlan).
- La configuration des interfaces de niveau 2 puis leur rattachement à leur VLAN secondaire et primaire.
- La configuration du port *promiscuous* et son rattachement au VLAN primary ainsi qu'aux VLAN secondaires.

© ENI Editions - All rigths reserved - Moha Anisa

Afin d'illustrer cette description, nous présentons un exemple de configuration réalisé sur un switch Cisco Catalyst 2980G utilisant le système d'exploitation CatOS. Dans les captures d'écran qui suivent, nous avons conservé les réponses du système et quelques retours de l'aide en ligne.

```
sw1> (enable) set vtp mode transparent
VTP domain  modified

switch> (enable) set vlan 10 pvlan-type primary name VLAN_PRIMAIRE
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 10 configuration successful


switch> (enable) set vlan 11 pvlan-type ?
  primary                   Set private vlan as primary vlan
  isolated                  Set private vlan as isolated vlan
  community                 Set private vlan as community vlan
  none                      Set vlan to be a normal vlan
  twoway-community          Set private vlan as twoway community
vlan
switch> (enable) set vlan 11 pvlan-type isolated name ISOLATED_1
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 11 configuration successful
```

- Le switch est tout d'abord mis en mode VTP transparent qui laisse passer les informations de ce protocole sans en tenir compte.

- Le VLAN primary est créé. Il porte le numéro 10 et le nom « VLAN_PRIMAIRE ».

- Un VLAN secondaire de type *isolated* est à son tour créé. Il porte le numéro 11 et le nom ISOLATED_1

```
switch> (enable) set vlan 12 pvlan-type isolated name ISOLATED_2
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 12 configuration successful
switch> (enable) set vlan 13 pvlan-type isolated name ISOLATED_3
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 13 configuration successful
switch> (enable) set vlan 14 pvlan-type community name COMMUNAUTE_1
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 14 configuration successful
switch> (enable) set vlan 15 pvlan-type community name COMMUNAUTE_2
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 15 configuration successful
```

Quelques autres VLAN secondaires sont créés.

```
switch> (enable) set pvlan 10 11
Vlan 11 configuration successful
Successfully set association between 10 and 11.

switch> (enable) set pvlan 10 12
Primary private vlan already has an isolated vlan associated.
Failed to set association between 10 and 12.

switch> (enable) set pvlan 10 13
Primary private vlan already has an isolated vlan associated.
Failed to set association between 10 and 13.

switch> (enable) set pvlan 10 14
Vlan 14 configuration successful
Successfully set association between 10 and 14.
```

© ENI Editions - All rigths reserved - Moha Anisa

Les VLAN secondaires sont associés au VLAN *primary*. Notons que les VLAN 12 et 13 ne peuvent pas être associés au VLAN *primary* car ce dernier est déjà associé au VLAN 11.

```
switch> (enable) show pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
10      11        isolated
10      14        community
10      15        community
-       12        isolated
-       13        isolated
```

La commande `show pvlan` nous montre les trois VLAN rattachés au VLAN *primary*.

```
switch> (enable) set pvlan 10 11 2/22-32
Successfully set the following ports to Private Vlan 10,11:
2/22-32

switch> (enable) sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
10      11        isolated         2/22-32
```

Quelques ports sont associés au VLAN *isolated* (et donc au VLAN *primary*).

```
switch> (enable) set pvlan mapping 10 11 2/17
Successfully set mapping between 10 and 11 on 2/17
```

Cette dernière commande de configuration déclare le port *promiscuous* et l'associe au VLAN *primary*.

```
switch> (enable) sh pvlan isolated
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
10      11        isolated         2/22-32

switch> (enable) sh pvlan mapping
Port Primary Secondary
---- ------- ---------
 2/17 10      11
```

Les deux commandes `sh pvlan isolated` et `sh pvlan mapping` nous montrent les ports dans le VLAN *isolated* et le port *promiscuous*.

Le port *promiscuous* est dans notre type de configuration connecté à un routeur afin de transmettre le trafic du VLAN vers le reste du réseau. Avec un switch fournissant des services de niveau 3, le port *promiscuous* aurait été affecté à une interface VLAN.

Afin d'atteindre cet objectif d'isolation entre les ports sur un modèle de switch ne disposant pas de la fonction *private VLAN*, nous avons sur un switch modèle 2950 utilisé la commande `switchport protected` en mode de configuration d'une interface.

```
SW0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW0(config)#int f0/3
SW0(config-if)#switchport protected
SW0(config-if)#end
SW0#
```

Notez au passage que la commande `end` permet de passer directement du mode de configuration au mode `exec`.

Il existe, comme souvent, une méthode permettant de contourner l'isolement dans le cas où une porte de sortie existerait via un routeur ou une interface VLAN. Une interface VLAN est une interface virtuelle recevant une adresse IP, elle est membre à part entière du VLAN et permet de le connecter au reste du réseau. Tout en respectant les principes de cette technologie, que se passe-t-il si nous adressons des paquets IP (destinés à un autre réseau) vers l'interface VLAN ?

Le routeur accomplira sa tâche et adressera le paquet vers l'adresse IP de destination réduisant à néant la protection précédemment mise en place. Afin de rétablir nos exigences initiales, il faut configurer le routeur avec une ACL de niveau 3 pour rejeter le trafic en provenance et à destination du réseau IP du *private VLAN*.

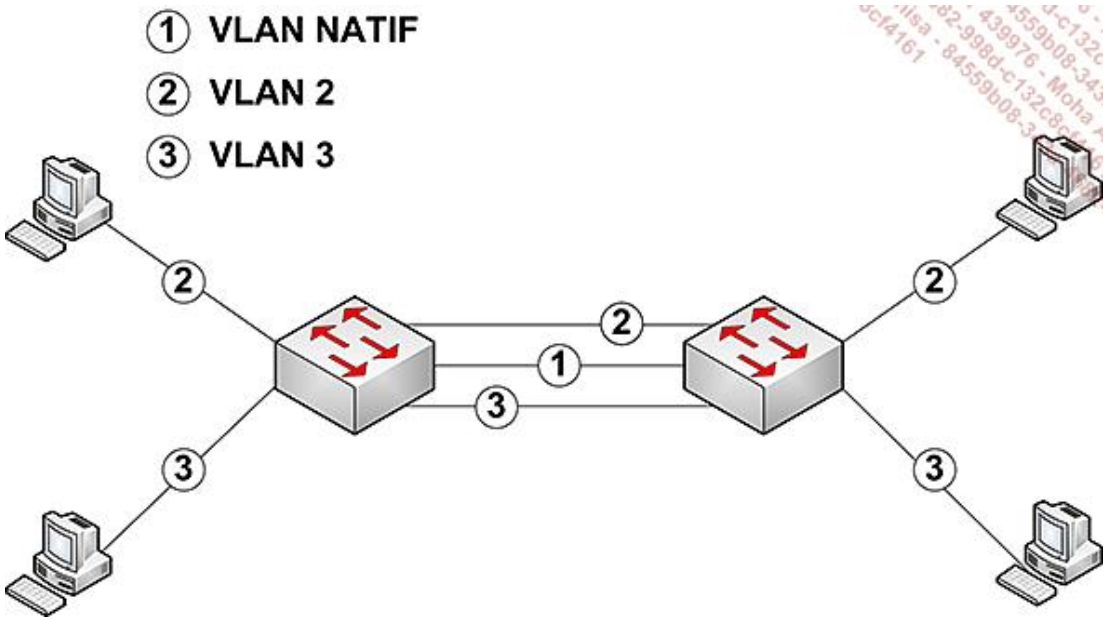
© ENI Editions - All rigths reserved - Moha Anisa

Envoyer vers l'interface VLAN signifie envoyer le trafic vers l'adresse de niveau 2 de l'interface VLAN.

Prévenir les changements de VLAN

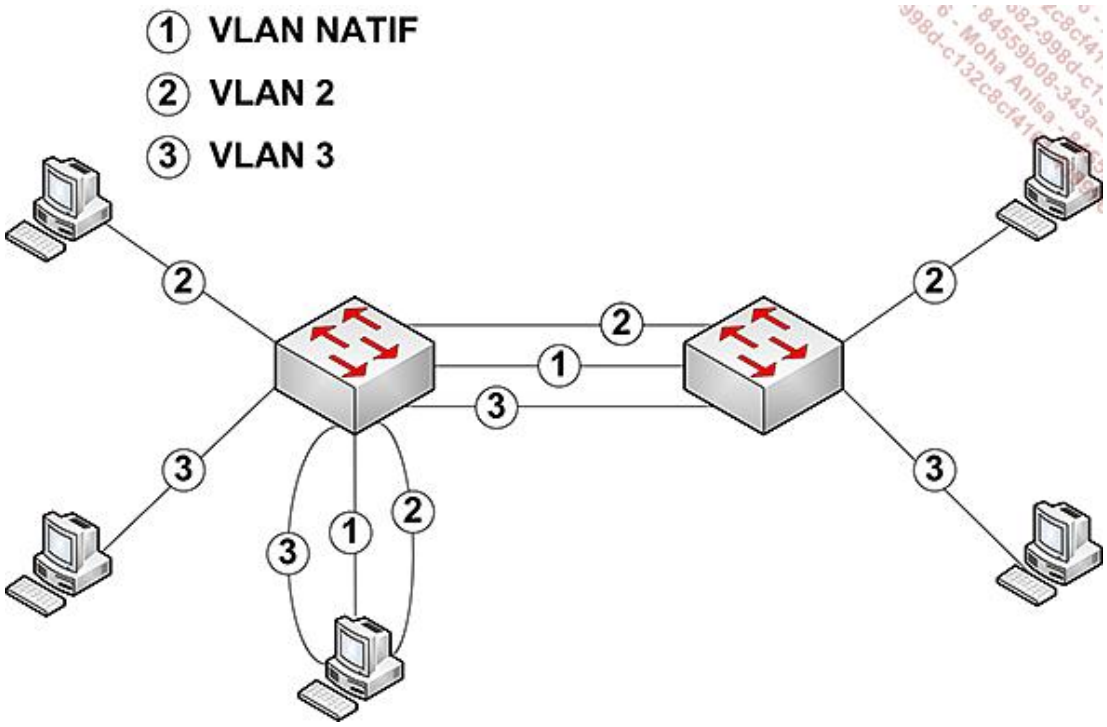
Un réseau commuté peut héberger de nombreux VLAN. Ils sont locaux (valides sur un seul switch) ou propagés entre plusieurs switch. Dans le premier cas (VLAN local) un PC dans le VLAN 2 du switch A ne pourra pas communiquer avec un PC membre du VLAN 2 sur le switch B. Dans le second cas, le VLAN 2 est disponible des deux côtés.

Lorsque les VLAN sont propagés de switch en switch, le passage d'un VLAN à un autre constitue une atteinte à la sécurité. Examinons le schéma suivant :



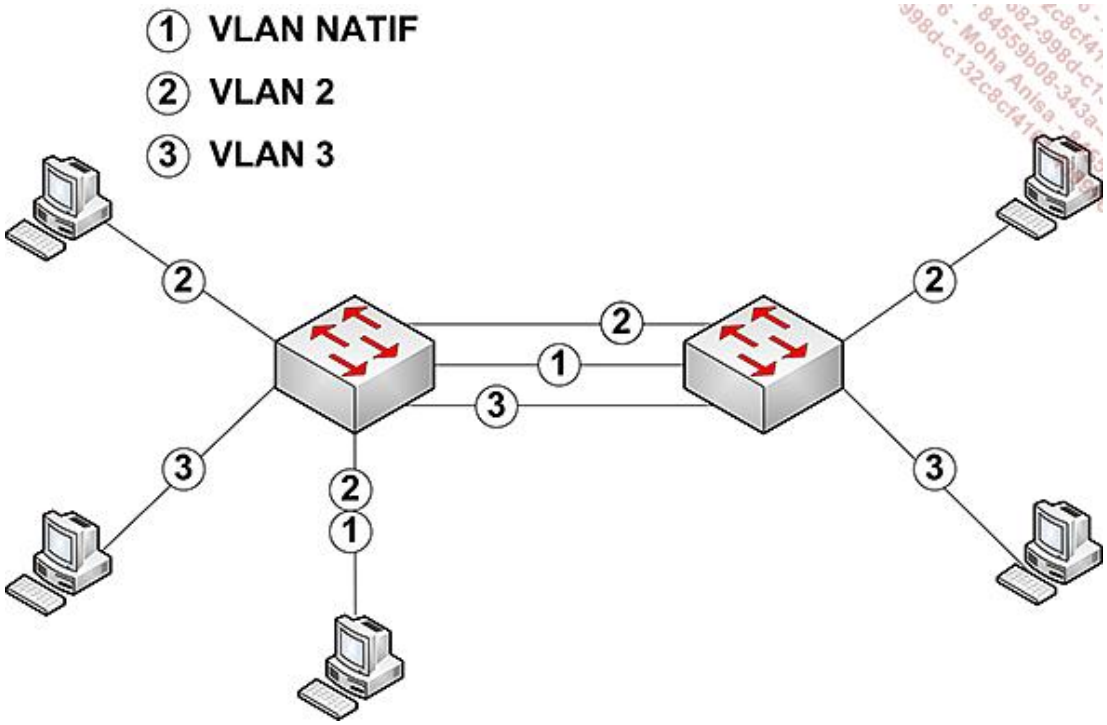
Les trois brins entre les deux switch portent le nom de *trunk*. Il s'agit d'un lien logique sur lequel transitent les paquets marqués comme appartenant aux divers VLAN. Un trunk est physiquement contenu sur un média unique (câble, fibre).

Deux types d'attaques existent.



La première consiste pour une station à prendre la place d'un switch et de se former un *trunk*. La station obtient ainsi ses entrées dans les VLAN. Cette attaque est connue sous le nom d'attaque DTP (*Dynamic Trunk Protocol*).

© ENI Editions - All rigths reserved - Moha Anisa



La seconde, plus élaborée consiste à forger un paquet qui sera marqué avec deux identifiants de VLAN en l'occurrence le VLAN natif du *trunk* et le VLAN dans lequel on souhaite pénétrer. Le trafic qui transite dans le VLAN natif n'est pas marqué, le second switch reçoit le paquet et ne voit que la marque 2 car la marque 1 n'est pas préservée lors du passage dans le *trunk*. Il met donc ce paquet dans le VLAN numéro 2. Un saut de VLAN est ainsi réalisé. Il faut pour mener à bien cette attaque que la machine à l'origine de celle-ci soit connectée sur le VLAN correspondant au VLAN natif du switch. Des outils comme *Scapy* ou *Yersinia* sont idéaux pour ce genre d'attaque.

Les parades disponibles sont très simples à mettre en œuvre. Il suffit de planifier avec précaution :

- La configuration des VLAN sur les ports en prenant soin de ne jamais affecter à un port le VLAN natif du *trunk*.
- La configuration des ports destinés à recevoir des machines. Ils seront forcés à ne jamais devenir des ports de type *trunk* avec la commande : `switchport mode access`.
- De ne jamais placer de ports dans le VLAN 1.

d. Lutter contre les serveurs DHCP indésirables

La découverte d'un serveur DHCP (*Dynamic Host Configuration Protocol*) non déclaré va de pair avec la soudaine déconnexion du réseau de plusieurs machines. Une première enquête sur le terrain révèle que les adresses IP des machines isolées ne sont pas issues des étendues habituelles. Une inspection plus approfondie (avec la commande `ipconfig /all`) montre que le serveur DHCP ayant délivré ces adresses dépend du domaine *mshome.net* lequel est inconnu. L'enquête se poursuit par une inspection des tables CAM à la recherche du port où cet indésirable serveur se trouve connecté. Après une remontée de câblage sans doute fastidieuse, l'intrus est enfin démasqué. Il s'agit d'un ordinateur portable voyageant régulièrement entre le réseau de l'entreprise et le domicile de son propriétaire où il est connecté à une ligne ADSL qu'il partage à loisir avec toute la maison et pourquoi pas le voisinage.

Ce cas constitue un déni de service involontaire et une personne mal intentionnée réussissant à installer un serveur DHCP pirate sur le réseau et déclarant une station sous son contrôle comme étant la passerelle par défaut pourra voir passer le trafic des stations leurrées. Cette attaque par interposition dans le flux porte en anglais le nom de *man in the middle*. Une autre attaque consiste à vider la réserve d'adresses IP du serveur DHCP par des demandes incessantes provenant d'une ou plusieurs machines sous le contrôle de la personne mal intentionnée.

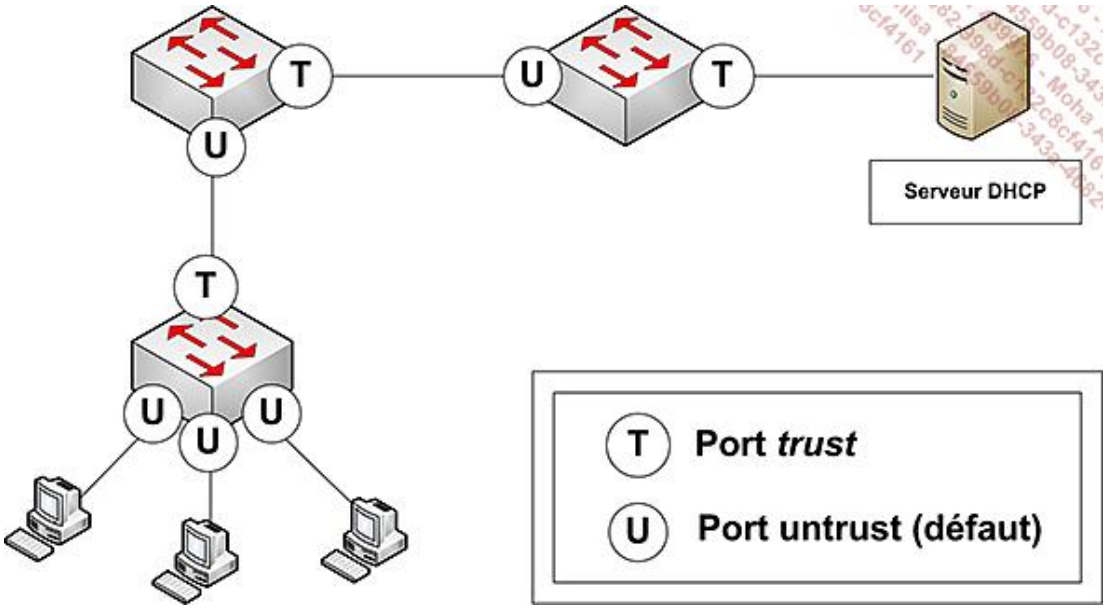
Le premier incident est assez fréquent sur un réseau qui ne met pas en œuvre les protections adéquates. En outre, la connexion sur le réseau d'une machine itinérante soulève bien d'autres questions. Comme toujours, les solutions existent et sont une fois de plus fort simples. Quelques commandes permettent sur les ports réservés aux utilisateurs de filtrer ce qui de près ou de loin ressemble à des messages provenant d'un serveur DHCP. Cette technique porte le nom de *DHCP Snooping*.

Le principe de base du *DHCP Snooping* est de considérer que sur un port quelconque aucun message du type de ceux émis par un serveur DHCP ne doit transiter. En revanche, les messages DHCP normalement émis par une station sont autorisés à transiter. Avec *DHCP Snooping*, le switch construit une table de correspondance entre les

© ENI Editions - All rigths reserved - Moha Anisa

adresses MAC, les adresses IP délivrées et les ports physiques. Cette table est également exploitée par la technologie *Dynamic Arp Inspection* dans le cadre de la détection de tentatives d'usurpation d'adresses MAC (mac spoofing).

Un port est configuré comme étant du type *trust* s'il est connecté directement ou indirectement à un serveur DHCP. Il est donc primordial d'étudier la chaîne des switch et les positions des ports *trust* afin d'assurer la pérennité de la configuration. Signalons enfin que les ports sont par défaut de type *untrust*.



Voici la configuration.

```
SW0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.

SW0(config)#ip dhcp snooping
SW0(config)#ip dhcp snooping vlan 2
SW0(config)#
SW0(config)#^Z
```

La fonctionnalité s'active une fois en mode global puis pour chacun des VLAN à protéger.

```
SW0#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
2
Insertion of option 82 is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
```

Une commande `show` donne un premier aperçu.

```
SW0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW0(config)#int f0/1
SW0(config-if)#ip dhcp snooping trust
SW0(config-if)#ip dhcp snooping limit rate 100
```

Le port f0/1 est configuré (*trust*) afin que *DHCP snooping* laisse passer les messages issus d'un serveur directement ou indirectement connecté, la commande `limit rate` autorise seulement 100 messages du protocole DHCP par seconde. Attention à bien étudier au préalable la quantité de messages devant transiter sur le lien afin de ne pas la sous-évaluer et entraîner un déni de service.

```
SW0# sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
2
Insertion of option 82 is enabled
Interface                    Trusted     Rate limit (pps)
```

© ENI Editions - All rigths reserved - Moha Anisa

```
-----------------------     -------     ----------------
FastEthernet0/1             yes         100

SW0# sh ip dhcp snooping binding
Option 82 on untrusted port is not allowed
MacAddress  IpAddress        Lease(sec)  Type     VLAN  Interface
----------  ---------------  ----------  -------  ----  ----------
x:x:x:19:03 10.xxx.xxx.x60   172724      dynamic  2
FastEthernet0/12
```

La commande `sh ip dhcp snooping` montre que l'interface f0/1 est la seule autorisée à faire transiter les messages DHCP issus d'un serveur. Quant à la commande `sh ip dhcp snooping binding`, elle montre le port f0/12 et l'adresse MAC de la station connectée. Cette table est exploitée pour analyser les messages DHCP à venir.

e. Lutter contre les interceptions

Ici, le protocole ARP (*Address Resolution Protocol*) est directement mis en cause ou plus exactement son implémentation sur les systèmes d'exploitation. ARP est chargé de résoudre et de maintenir une table des couples adresse IP et adresse MAC. Les messages du protocole ARP cherchent à quelle adresse de niveau 2 correspond une adresse de niveau 3, le but est de trouver la carte réseau vers laquelle envoyer les trames de niveau 2 qui contiennent l'information à transmettre. Un dialogue typique des échanges ARP est le suivant :

- À quelle adresse MAC dois-je envoyer le trafic destiné à l'adresse IP 192.168.0.1 ? (ce message est recopié sur tous les ports du swich)
- Je suis l'adresse IP 192.168.0.1 et mon adresse MAC est la suivante : 00.18.ab.cd.ab.cd (ce message est transmis directement).

L'administrateur d'un système peut également renseigner manuellement la table ARP.

```
C:\Users\RZS>arp -a

Interface: 10.xxx.xxx.x66 --- 0xb
  Internet Address      Physical Address      Type
  10.xxx.xxx.x          00-02-b3-95-e4-4e     dynamic
  10.xxx.xxx.x          00-b0-d0-ec-8d-a4     dynamic
  10.xxx.xxx.x          00-0c-29-48-bd-64     dynamic
  10.xxx.xxx.x          00-0e-7f-3e-57-83     dynamic
  10.xxx.xxx.x          00-0d-02-d1-64-65     dynamic
  10.xxx.xxx.x          00-16-d4-ee-df-4d     dynamic
  10.xxx.xxx.x          00-0f-fe-77-2d-3f     dynamic
  10.xxx.xxx.x          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
```

Voici la table ARP d'une machine Windows.

Un message ARP important est le message ARP gratuit (*gratuitous ARP*). Ce message est émis au démarrage par un hôte qui cherche à savoir si une adresse IP identique à la sienne existe déjà. Cette requête est reçue par tous les hôtes à l'écoute qui mettent à jour (avec l'information reçue) leur propre table ARP. Le protocole ARP ne possédant pas de mécanisme d'authentification, les hôtes d'un sous-réseau prennent en compte les messages qui leur sont adressés même s'ils n'ont rien demandé.

Le principe des attaques ARP consiste à envoyer régulièrement vers la machine à tromper soit des messages ARP gratuits, soit des messages répondant à une demande qui n'a jamais été effectuée. L'hôte victime, à la réception des messages provenant de la machine de l'attaquant met à jour sa table ARP sans autre forme de procès. L'attaquant fait ainsi croire à ses victimes qu'il est par exemple la passerelle par défaut et si l'attaque aboutit, les communications des victimes à destination de l'extérieur du sous-réseau passeront par lui.

Les switch sont vulnérables à ce genre d'attaques car les tables d'états ne tiennent pas compte du couple adresse MAC - adresse IP, mais du couple adresse MAC - port.

Il est toujours possible de fixer les couples MAC - IP de manière statique, mais sur un réseau de grande dimension la tâche s'avère quasi impossible. Un dispositif automatique doit donc prendre en charge la vérification de la pérennité des couples adresse MAC - adresse IP et surveiller tout changement anormal. Un programme comme *Arpwatch* disponible sous Linux se charge de cette tâche et renseigne un fichier avec les couples découverts et les changements éventuels. Le programme dispose d'une option pour avertir par courriel l'administrateur.

```
    ethernet vendor: Compaq (HP)
          timestamp: Friday, April 18, 2008 11:28:23 +0200
```


© ENI Editions - All rigths reserved - Moha Anisa

```
From: arpwatch (Arpwatch TestStation)
To: root
Subject: new station (xx.xxx.xxxxxxx.xxxxx.net) eth0

            hostname: xx.xxx.xxxxxxx.xxxxx.net
          ip address: 10.yyy.yyy.yyy
           interface: eth0
    ethernet address: 0:b0:d0:xx:xx:xx
     ethernet vendor: Dell Computer Corp.
           timestamp: Friday, April 18, 2008 11:28:40 +0200
```

Voici un bref extrait du fichier dans lequel le programme écrit les couples qu'il découvre en écoutant le sous-réseau. Pour mémoire, le champ *ethernet vendor* est déduit à partir de la première moitié de l'adresse MAC.

```
Apr 18 15:20:16 TestStation arpwatch: changed ethernet address
10.xxx.xxx.xxx 0:17:42:xx:xx:xx (0:b:5d:xx:xx:xx) eth0
```

Ce message montre un changement d'adresse MAC pour une adresse IP précédemment connue.

Installer un dispositif comme *Arpwatch* pour chaque sous-réseau nécessite la mise à disposition de machines dédiées. De plus, les nombreux messages doivent être exploités à la recherche des changements suspects. Enfin, *Arpwatch* ne prend aucune décision lorsqu'il constate un changement.

Cisco offre une solution de surveillance des couples adresse MAC - adresse IP baptisée DAI (*Dynamic Arp Inspection*). Cette fonctionnalité s'appuie sur les services que nous avons utilisé pour protéger les serveurs DHCP. Plus précisément, DAI lorsqu'il est activé recherche dans la table du *DHCP snooping* les couples valides. Si l'environnement réseau n'est pas configuré en DHCP, DAI se réfère à une ACL ARP (filtrage sur les adresses MAC).

Les ACL ARP sont prioritaires sur la table du *DHCP snooping*. Si une ACL est placée dans la configuration et associée à un VLAN, le rejet implicite (*deny*) à la fin de l'ACL bloquera le trafic non autorisé même si ce dernier est inscrit dans la table du *DHCP snooping*.

Les étapes de la configuration de DAI sont simples. Quelques précautions sont à prendre si la politique de sécurité impose une limitation du nombre de messages ARP sur un temps donné, si les interfaces sont en *port-channel* ou en *trunk*. Un dépassement de la limite entraînant alors un rejet du trafic.

Examinons la configuration de DAI.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 2
Switch(config)#ip arp inspection vlan 2
```

Nous activons les fonctions *DHCP snooping* et *DAI* dans le VLAN2 en prenant bien soin d'activer *DHCP snooping* globalement.

```
Switch(config)#int f0/1
Switch(config-if)#ip arp inspection trust
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#end
```

Comme nous l'avions fait pour *DHCP snooping*, nous déclarons une interface derrière laquelle nous savons qu'un serveur DHCP licite est connecté directement ou indirectement.

```
00:23:13: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/2,
vlan 2.([0018.8b7e.20e9/10.xxx.xxx.212/0000.0000.0000/10.xxx.xxx.153/00:23:12
UTC Mon Apr 12 2008])
```

Considérons le cas où notre switch (un modèle 3550) regroupe des machines non configurées avec le protocole DHCP. Le switch détecte sur l'interface *FastEthernet 0/2* une machine qui ne figure ni dans la table du *DHCP snooping* ni dans une ACL ARP. Ce message est affiché grâce à la commande `logging console` en mode global. Afin que son trafic puisse traverser le VLAN, il faut configurer une *ACL* de niveau 2 comme suit :

```
Switch(config)#arp access-list ARP-ACL-TEST
Switch(config-arp-nacl)#?
Extended ARP Access List configuration commands:
  default  Set a command to its defaults
  deny     Specify packets to reject
  exit     Exit ACL configuration mode
  no       Negate a command or set its defaults
```

© ENI Editions - All rigths reserved - Moha Anisa

```
  permit   Specify packets to forward
```

On entre dans le mode de configuration et on donne un nom à l'access-list.

```
Switch(config-arp-nacl)#permit ip host 10.xxx.xxx.212 mac
0018.8Bxx.xxxx 0.0.0
```

Cette commande (sans le retour à la ligne) associe l'adresse IP 10.xxx.xxx.212 à l'adresse MAC 0018.8Bxx.xxxx. 0.0.0 est un masque pour l'adresse MAC qui signifie : « cette adresse précisément ».

```
Switch(config)#ip arp inspection filter ARP-ACL-TEST vlan 2
```

Pour terminer, l'ACL *ARP-ACL-TEST* est appliquée au VLAN (le VLAN 2 dans notre cas).

Comme nous l'avons souligné, cette ACL est prioritaire. C'est pourquoi il est recommandé de ne pas mélanger sur un même sous-réseau des machines utilisant et n'utilisant pas le protocole DHCP.

Si nous considérons un réseau entièrement configuré avec DHCP, une station requiert une adresse IP et la reçoit d'un serveur. Au passage, DHCP snooping renseigne sa table. Rappelons que ce serveur est au bout de la chaîne des ports déclarés *trust*.

```
Switch#sh ip dhcp snooping binding

MacAddress          IpAddress        Lease(sec)  Type           VLAN
Interface
------------------  ---------------  ----------  -------------  ----
--------------------
00:0B:5D:xx:xx:xx   10.xxx.xxx.152   172769      dhcp-snooping  2
FastEthernet0/3
Total number of bindings: 1
```

La commande `sh ip dhcp snooping binding` montre la table dans laquelle se trouvent les couples surveillés. En cas de changement, DAI rejette le trafic issu de la machine incriminée.

f. Résumé

Nous avons au cours de ce chapitre passé en revue les principales mesures de protection des deux premières couches du modèle OSI.

- La protection physique des équipements et de l'accès au réseau est un point crucial car aucune attaque ne saurait être menée sans connexion.
- Le raccordement au port physique d'un switch est sécurisé tant au niveau physique que logique. À cet effet, les techniques 802.1X ainsi que la limitation des adresses MAC par port sont à considérer.
- Les VLAN ne sont plus la panacée, il convient de relever leur niveau de sécurité avec des techniques comme les *Private VLAN*, les *VLAN ACL* (*VACL*). De plus, dans le cas d'un *trunk* entre deux switch, il est indispensable de se prémunir contre toute possibilité de changement intempestif de VLAN.
- Les switch offrent une isolation du trafic port à port (comparativement à un concentrateur) mais sont vulnérables si la table des couples adresses MAC - port est saturée ou corrompue. À chaque port correspond un nombre minimal d'adresses MAC nécessaire au bon fonctionnement du dispositif connecté (PC seul ou PC et Téléphone IP).
- Les serveurs DHCP installés sans autorisation sur un sous-réseau entrainent des dénis de services. La technologie *DHCP snooping* permet de se prémunir contre ce genre d'accident.
- Les switch dans leur configuration par défaut ne protègent nullement les systèmes d'exploitation contre la corruption de leurs propres caches ARP. Cependant, la technologie *Dynamic Arp Inspection* pallie à cet état de fait en inspectant et en surveillant les couples adresse MAC - adresse IP (avec l'aide de *DHCP snooping*).

Pour clore ce chapitre, nous ajoutons une mesure de sécurité reprise sur le chapitre traitant des protections globales d'un équipement Cisco. Le protocole CDP (*Cisco Discovery Protocol*) se situe au niveau deux et présente quelques risques s'il est activé. S'il n'est pas nécessaire au bon fonctionnement du réseau, il est fortement conseillé de le désactiver.

© ENI Editions - All rigths reserved - Moha Anisa

Conclusion

Nous venons d'examiner les menaces et les mesures de protection qui permettent de garantir la sécurité des deux premières couches de modèle OSI. La sécurité commence ici avec un strict contrôle de l'accès aux médias que sont les réseaux câblés (filaire ou optique). Nous aborderons dans un prochain chapitre ce même thème appliqué cette fois aux réseaux sans fils qui utilisent les ondes radioélectriques comme média. La seconde couche du modèle OSI a la responsabilité d'acheminer les communications entre des hôtes partageant un même média, à ce titre elle est la cible de nombreuses attaques visant à détourner le trafic vers des tiers ayant au préalable usurpé des adresses physiques. Cette couche est également victime d'attaques ayant pour objectif la saturation des mémoires réservées au stockage de ces mêmes adresses.

Avec l'extension des réseaux d'entreprise, le besoin s'est fait sentir d'isoler les segments les uns des autres afin de restreindre les domaines de collision au niveau de la couche 2. Cette exigence est accomplie par les VLAN qui, nous l'avons vu, ne garantissent pas une isolation suffisante. De même, à l'intérieur des VLAN, un autre niveau d'isolation est parfois requis afin que les membres d'un segment ne puissent pas communiquer entre eux.

La sécurité de la couche 2 est primordiale car les mesures de protection appliquées aux couches supérieures peuvent dépendre étroitement des couches inférieures.

Le chapitre suivant nous propulse deux couches plus haut vers les niveaux trois et quatre dans l'univers de TCP/IP.

© ENI Editions - All rigths reserved - Moha Anisa

Notions sur la couche 3

Au niveau de la couche 3 du modèle OSI, les équipements terminaux reçoivent en plus de leur adresse physique (propre à la couche 2) une adresse dite logique. Les machines qui sont connectées à un réseau et qui doivent échanger des données ne sont pas toutes obligatoirement sur le même segment physique et n'ont donc pas une vue directe les unes des autres lors de la mise en œuvre des protocoles de niveau 2 (comme ARP) que nous avons évoqué au chapitre précédent. Il est donc nécessaire d'utiliser un autre niveau pour communiquer en s'affranchissant des barrières. Ainsi naquit Internet qui offre de nos jours la possibilité à tout un chacun d'échanger des informations avec des correspondants lointains. Une analogie très souvent employée et fort à propos est celle du téléphone. Il est en effet aisé d'aborder les concepts d'adressage et de segmentation en les comparant avec la manière dont les numéros de téléphone sont organisés par pays, par région, par central téléphonique urbain et par répartiteur dans chaque quartier. Cette chaîne hiérarchique est utilisée pour localiser les correspondants en vue d'établir la communication (et de la facturer). Il en est de même pour les adresses IP qui possèdent des propriétés utilisées par les architectes afin de segmenter les réseaux. Une fois physiquement et logiquement séparés, les équipements terminaux utilisent les services offerts par d'autres équipements afin de communiquer en s'affranchissant de la segmentation. Ces équipements sont connus sous le nom de routeurs.

Cependant, si rien n'est fait, le réseau acheminera aveuglément les données pourvu qu'une route (un chemin) existe entre tous les participants. Si le but espéré est atteint en terme de communication hors des limites physiques du réseau local, il n'en est pas de même en matière de sécurité (aux exigences près). Du point de vue sécuritaire, la couche 3 et le protocole TCP/IP en particulier offrent une gamme de services dont les objectifs premiers sont justement de faciliter les communications dans un univers très large où la confiance règne. Ce monde parfait n'existe hélas pas et les réseaux ouverts aux partenaires honnêtes le sont aussi aux pirates de tout poil.

Avant de poursuivre, et de poser nos exigences de sécurité, admettons comme postulat de départ que les réseaux sont de deux types : internes et externes. Cette distinction est la conséquence directe du manque d'adresses publiques pour les équipements IP.

© ENI Editions - All rigths reserved - Moha Anisa

Exigences de sécurité

Comme pour le chapitre précédent, nous allons exposer les exigences de sécurité qui rappelons-le sont des contraintes à respecter dans le cadre de la politique de sécurité. Nous partons cette fois du principe que les exigences revêtent un caractère obligatoire. Les exigences sont mises directement en correspondance avec la technique.

Exigences de sécurité de l'équipement réseau pour la couche 3	
Exigences	**Technique**
Disposer d'une redondance IP sûre pour la route par défaut.	HSRP
Filtrer le trafic entre réseaux IP en tenant compte des connexions et de leur sens.	Context-Based access control ACL
Se protéger des attaques TCP.	TCP Intercept
Préserver la confidentialité et l'intégrité des échanges.	IPSec
Sécuriser les protocoles de routage.	Contrôles embarqués dans les protocoles
Séparer les adresses internes des adresses publiques tout en assurant la correspondance entre elles.	Adresses RFC 1918

© ENI Editions - All rigths reserved - Moha Anisa

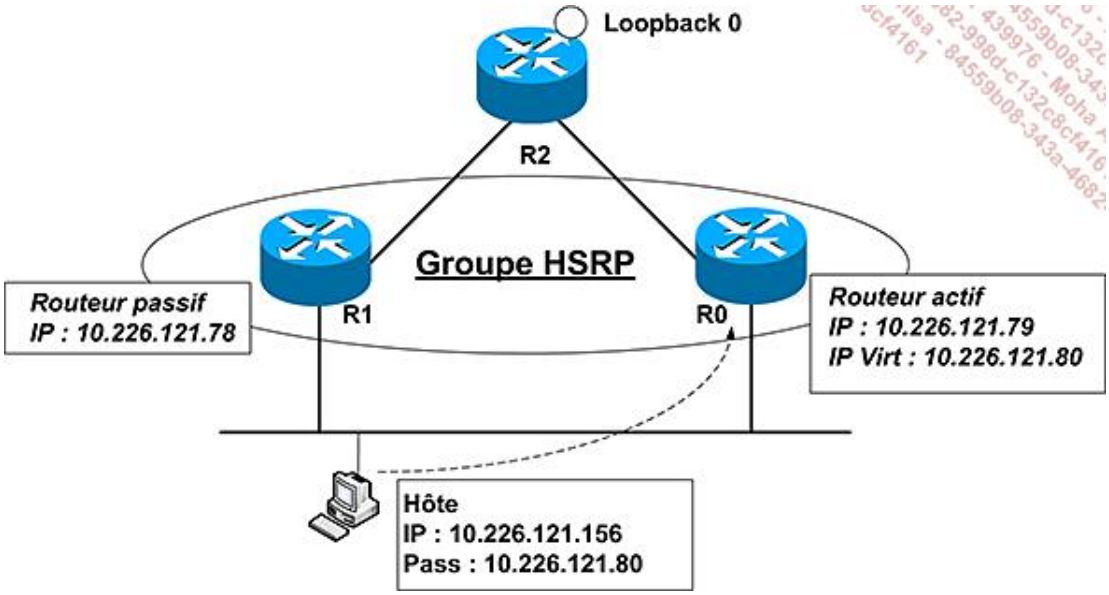
Le protocole HSRP

L'objectif à atteindre est de disposer d'une sureté de fonctionnement renforcée sur une passerelle IP dont la disponibilité est primordiale.

Il est à proprement parler délicat de prêter au protocole HSRP une fonction de sécurité au sens strict, toutefois sous la perspective de la sécurité de fonctionnement, le protocole HSRP assure des fonctions intéressantes et embarque un contrôle de sécurité. Le protocole HSRP offre ainsi, avec au minimum deux routeurs, des possibilités de recouvrement.

Le principe de fonctionnement de HSRP est simple à comprendre. Les routeurs membres d'un même groupe HSRP sont connectés sur un brin physique commun. Ils sont configurés de telle manière qu'un seul d'entre eux réponde à l'adresse IP de passerelle par défaut déclarée sur les stations de travail. En cas d'indisponibilité du routeur actif, le routeur passif prend le relais. Lorsque l'ancien routeur actif redevient disponible, il peut en fonction de la configuration reprendre sa place de routeur actif ou demeurer passif. Les deux routeurs se partagent donc la gestion d'une adresse IP virtuelle (VIP) tout en gardant leurs adresses propres.

Le protocole HSRP est capable de déclencher une bascule de l'adresse virtuelle si l'une des interfaces externes ne fonctionne plus. Ceci concerne l'interface physique (*line protocol down*) et non la disparition d'une route. Enfin, signalons que le protocole HSRP offre une fonction d'authentification mutuelle grâce à l'échange de messages hachés en MD5. HSRP est disponible en deux versions. Examinons à présent une configuration type.



La station de travail possède une adresse de passerelle par défaut pointant sur l'adresse virtuelle générée par les routeurs R0 et R1 qui implémentent le protocole HSRP. Ces deux routeurs sont connectés au routeur R2 qui possède une interface de bouclage (dite de *loopback*). Le but est de conserver la connectivité de la station de travail vers l'interface de bouclage (*loopback 0*) via l'un des deux routeurs HSRP (R0 ou R1) et ce, de manière transparente. Nous rappelons qu'une interface de bouclage est une interface purement virtuelle et qui à ce titre est toujours présente (tant que le routeur est sous tension).

```
1 - interface FastEthernet0/0
2 - ip address 10.226.121.79 255.255.255.0
3 - duplex auto
4 - speed auto
5 - standby 0 ip 10.226.121.80
6 - standby 0 preempt
7 - standby 0 authentication md5 key-string 7 00071A150754
8 - standby 0 track FastEthernet0/1 30
```

Voici la configuration HSRP du routeur R0. Nous observons sur la ligne 5 l'adresse virtuelle qui sera cogérée avec R1 (10.226.121.80), le mot `preempt` sur la ligne 6 indique que R0 s'il venait à tomber en panne et à revenir en service reprendrait alors la gestion de l'adresse virtuelle. Séquence d'authentification entre les deux partenaires HSRP qui évite à un routeur indésirable d'entrer dans le groupe de gestion de cette adresse virtuelle.

```
1 - interface FastEthernet0/0
2 -  ip address 10.226.121.78 255.255.255.0
3 -  duplex auto
4 -  speed auto
5 -  standby 0 ip 10.226.121.79
6 -  standby 0 preempt
```

© ENI Editions - All rigths reserved - Moha Anisa

```
7 -  standby 0 priority 80
8 -  standby 0 authentication md5 key-string 7 00071A150754
```

La configuration de R1 montre sur la ligne 7 le mot `priority` 80 qui indique que le routeur R1 lors de la première négociation avec R0 (qui possède une `priority` de 100 par défaut) ne prendra pas le contrôle de l'adresse virtuelle. Notons la similitude des séquences d'authentification en md5.

HSRP dispose d'une option particulièrement intéressante en cas de panne non pas du routeur en lui-même mais d'une de ses interfaces. Imaginons sur le schéma précédent une coupure du lien entre R0 et R2. HSRP grâce à la commande `track` (voir la configuration de RO) va décrémenter la valeur de priorité (`priority`) du routeur R0 de telle sorte qu'elle soit inférieure à celle du routeur R1 qui prendra alors à son compte la gestion de l'adresse virtuelle. Dans notre cas, la valeur `priority` du routeur R0 passera de 100 à 70 grâce à la dernière ligne de commande de notre configuration. Observons les réactions des routeurs lors d'une bascule suite à l'arrêt de l'interface entre R0 et R2.

```
Fa0/0 Hello  out 10.226.121.78 Standby pri 80 vIP 10.226.121.79
Fa0/0 Hello  in  10.226.121.77 Active  pri 70 vIP 10.226.121.79

Hello rcvd from lower pri Active router (70/10.226.121.77)
Fa0/0 Nbr 10.226.121.77 no longer active for group 0 (Standby)
Fa0/0 Nbr 10.226.121.77 Was active
Fa0/0 Grp 0 Hello  out 10.226.121.78 Active pri 80 vIP
10.226.121.79
```

Sur cette capture tronquée pour plus de lisibilité nous observons la valeur `priority` du routeur R0 qui est de 70 après coupure de son interface vers R2. R1 (.78) prend donc gestion de l'adresse virtuelle (.79) avec une `priority` de 80.

```
C:\Users\RZS>ping 192.168.2.1 -t

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=6ms TTL=254
Reply from 192.168.2.1: bytes=32 time=6ms TTL=254
Reply from 192.168.2.1: bytes=32 time=6ms TTL=254
Reply from 10.226.121.77: Destination host unreachable.
Reply from 10.226.121.77: Destination host unreachable.
Reply from 10.226.121.77: Destination host unreachable.
Reply from 10.226.121.77: Destination host unreachable.
Reply from 10.226.121.77: Destination host unreachable.
Reply from 192.168.2.1: bytes=32 time=6ms TTL=254
Reply from 192.168.2.1: bytes=32 time=6ms TTL=254
Reply from 192.168.2.1: bytes=32 time=4ms TTL=254
Reply from 192.168.2.1: bytes=32 time=5ms TTL=254
Reply from 192.168.2.1: bytes=32 time=5ms TTL=254
Reply from 192.168.2.1: bytes=32 time=5ms TTL=254
Reply from 192.168.2.1: bytes=32 time=5ms TTL=254
```

Le test qui précède consiste à envoyer des PING vers l'adresse de bouclage de R2 en coupant le lien entre R0 et R2. L'adresse IP virtuelle bascule entraînant la perte de cinq paquets.

Il est tout à fait envisageable de créer des groupes HSRP multiples afin de répartir des groupements de machines sur plusieurs passerelles virtuelles.

© ENI Editions - All rigths reserved - Moha Anisa

Les ACL

L'objectif à atteindre est de disposer d'une fonction de filtrage prenant en compte l'historique des connexions en cours afin de ne pas accepter du trafic qui n'aurait pas été demandé à partir d'une zone précise du réseau.

Les listes de contrôle d'accès (en anglais Access Control List ou ACL) semblent avoir toujours existé sur les routeurs Cisco et rares sont les configurations où elles n'apparaissent pas. Les ACL servent principalement au filtrage des paquets sur les interfaces physiques cependant leur mode de définition est employé pour catégoriser les réseaux en vue, entre autre, de les injecter dans un protocole de routage ou de les soumettre à une règle de qualité de service. Les types d'ACL proposés sont les suivants :

- les ACL standards qui filtrent sur l'adresse source ;
- les ACL étendues qui filtrent sur l'adresse source, l'adresse destination ainsi que les ports sources et destination ;
- les ACL *lock and Key* se mettent en place après authentification de l'utilisateur (en telnet) ;
- les named ACL sont des ACL étendues qui reçoivent un nom au lieu d'un numéro ;
- les ACL *reflexives* utilisent les informations de session pour laisser entrer les paquets de retour correspondant aux paquets envoyés ;
- les *time-based* ACL sont actives sur une plage de temps donnée ;
- les ACL *Context-based access control* utilisent les informations de session pour autoriser à la demande et en fonction du sens d'initialisation le passage du trafic.

La définition des ACL dans une configuration est l'objet de très nombreux chapitres voire de livres entiers aussi nous ne traiterons pas ici tous les cas de figure mais une sélection concernant la sécurité.

1. ACL et politique de sécurité

Les ACL sont nécessaires pour l'implémentation de nombreux points de la politique de sécurité réseau. Résumons dans un tableau les exigences les plus courantes dans lesquelles les ACL sont sollicitées.

Communications vers les équipements du réseau
Seul les réseaux d'administration peuvent se connecter aux équipements sur les ports HTTPS, SSL et SNMP choisis.
Communications des équipements vers le réseau
Les équipements du réseau communiquent avec les réseaux d'administration sur les ports SYSLOG et TFTP.
Les équipements du réseau échangent les routes entre eux au sein du même groupe administratif avec le protocole OSPF.
Les équipements du réseau sur les interfaces WAN acceptent uniquement les protocoles de la suite de chiffrement IPSec.
Communications entre réseaux
Interdire au trafic Internet non sollicité d'entrer sur le réseau.
Filtrer le trafic entre les VLAN.
Filtrer le trafic en entrée et en sortie sur les fermes de serveurs.

© ENI Editions - All rigths reserved - Moha Anisa

Assurer l'ouverture dynamique des ports pour les communications VoIP.

Ce court tableau est ajustable en fonction des contraintes imposées par la politique de sécurité. Il est impératif d'y faire figurer la règle de déni implicite rejetant tout ce qui n'a pas été dument autorisé en sachant toutefois que c'est une règle incontournable sur les routeurs Cisco bien qu'elle n'apparaisse pas.

La règle de déni lorsqu'elle est intégrée à la fin d'une ACL est associée avec le mot "log" afin de garder une trace du trafic rejeté. Cette pratique est recommandée.

2. Les ACL étendues

Une ACL se compose de deux parties. La première opère une sélection et la seconde applique cette sélection à un processus.

Prenons l'exemple d'un trafic à filtrer sur une interface avec une ACL étendue :

- La sélection s'opère sur un quadruplet adresse source - adresse destination - port source - port destination.
- À ce quadruplet est joint le mot `permit` ou `deny` qui sélectionne ou ne sélectionne pas le trafic désigné.
- Dans le cas d'une ACL ayant vocation à filtrer le trafic sélectionné, le mot `permit` autorise le trafic à transiter et le mot `deny` le bloque.
- Une ACL peut contenir plusieurs séquences. Le trafic est comparé à chacune de ces séquences de manière descendante.
- Lorsqu'une correspondance est trouvée, la comparaison s'arrête et le trafic est autorisé à traverser l'interface ou rejeté (attention à ne pas insérer un `permit` universel au milieu de l'ACL).
- Un `deny` implicite (et invisible) est ajouté à la fin de chaque ACL.

L'exemple type du filtrage de paquets IP sur une interface physique ressemble à ceci : « interdire l'ouverture d'une session telnet sur l'adresse 192.168.2.1 ».

Dans un premier temps le trafic est identifié par la création d'une règle, puis cette règle est appliquée à une interface.

```
!
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 ip access-group No-Telnet-In in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
ip access-list extended No-Telnet-In
 deny tcp any host 192.168.2.1 eq telnet log
```

Toutefois, sur cet extrait de configuration la configuration de l'interface apparait avant. La règle décrite précédemment est appliquée ici. Notons à la fin de l'ACL le mot `log`.

```
R2#sh ip access-lists
Extended IP access list No-Telnet-In
    10 deny tcp any host 192.168.2.1 eq telnet log (1 match)
```

`Log` permet de garder une trace des paquets qui seront traités par l'ACL et en l'occurrence rejetés comme le montre le résultat de la commande `show ip access-lists`.

© ENI Editions - All rigths reserved - Moha Anisa

Les ACL Standard sont la forme la plus simple mise en œuvre sur les routeurs et le contrôle porte uniquement sur l'adresse source ou le réseau source.

```
R1(config)#access-list 10 permit 10.10.10.32 0.0.0.15
```

Ici, le réseau 10.10.10.32 est autorisé, en fonction de l'utilisation de l'ACL, à passer une interface, à être injecté dans un protocole dynamique par exemple. Comment trouver le chiffre 15 dans le masque inversé qui accompagne l'ACL ? Pour ceux qui ne connaissent pas l'astuce, la voici : avant de programmer cette ACL, vous savez que les adresses à autoriser sont du type 10.10.10.0 255.255.255.240. Combien vaut la différence entre 240 et 255 ? 15 ! Le tour est joué. Il est fortement recommandé de préparer à l'avance les ACL dans un éditeur de texte simple d'utilisation et de les copier-coller dans la fenêtre du terminal. N'oubliez pas d'ajouter un retour chariot après la dernière ligne pour la valider automatiquement. C'est également une bonne idée de penser à la sauvegarde sous forme de fichier texte de toutes vos ACL.

Les ACL étendues offrent la possibilité de classer les entrées avec des numéros de séquence.

```
R1#sh ip access-lists
Extended IP access list Filtrage
    10 permit tcp any host 192.168.1.1 eq domain
    20 permit tcp any host 192.168.2.2 eq www
    30 permit tcp any host 192.168.2.2 eq 443
    40 permit tcp any host 192.168.2.3 eq smtp
    50 permit tcp any host 192.168.2.3 eq pop3
```

Cet extrait de configuration montre une ACL étendue permettant l'accès à divers serveurs à partir de n'importe quel réseau source (`any`). Tentons à présent de réorganiser notre ACL pour faire remonter la ligne concernant le trafic POP3. Les ACL étant lues de manière séquentielle, il est primordial de positionner au plus haut les règles les plus utilisées. Ceci est valable pour tous les firewall fonctionnant de la sorte.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list extended Filtrage
R1(config-ext-nacl)#no 50 permit tcp any host 192.168.2.3 eq pop3
R1(config-ext-nacl)#15 permit tcp any host 192.168.2.3 eq pop3
R1(config-ext-nacl)#^Z
R1#sh ip access-lists
Extended IP access list Filtrage
    10 permit tcp any host 192.168.1.1 eq domain
    15 permit tcp any host 192.168.2.3 eq pop3
    20 permit tcp any host 192.168.2.2 eq www
    30 permit tcp any host 192.168.2.2 eq 443
    40 permit tcp any host 192.168.2.3 eq smtp
```

Nous réorganisons l'ACL en annulant dans un premier temps la séquence 50 et en la repositionnant sous le numéro 15. Elle passe ainsi en seconde position.

Si d'aventure un incrément de 5 était souhaité à partir du premier numéro de séquence (en l'occurrence 10), il nous faudrait utiliser la commande `resequence` comme suit.

```
R1(config)#ip access-list resequence Filtrage 10 5
R1(config)#^Z
R1#sh ip access-lists
Extended IP access list Filtrage
    10 permit tcp any host 192.168.1.1 eq domain
    15 permit tcp any host 192.168.2.3 eq pop3
    20 permit tcp any host 192.168.2.2 eq www
    25 permit tcp any host 192.168.2.2 eq 443
    30 permit tcp any host 192.168.2.3 eq smtp
```

Il est très facile d'introduire une erreur dans une ACL. La pire de toute est de se « couper la patte » c'est-à-dire de mettre fin à sa propre session ce qui est fâcheux sur un accès distant lorsque l'on ne dispose pas d'un chemin alternatif. La commande `reload` offre la possibilité de programmer le redémarrage d'un routeur. La façon de procéder est la suivante :

- Lancement de la commande `reload` assortie d'un certain délai pour lancer le redémarrage.

© ENI Editions - All rigths reserved - Moha Anisa

- Le travail à effectuer.
- Si tout est correct : annulation de la commande `reload (reload cancel)` et sauvegarde de la configuration.
- En cas de coupure intempestive, le routeur redémarrera sur sa configuration précédente.

```
R1#reload in ?
Delay before reload (mmm or hhh:mm)

R1#reload in 15

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Reload scheduled in 15 minutes by vty0 (10.226.121.161)
Reload reason: Reload Command
Proceed with reload? [confirm]
R1#
R1# !------“commandes à passer au routeur”------!
R1# !------“commandes à passer au routeur”------!
R1# !------“commandes à passer au routeur”------!

R1#reload cancel
R1#


***
*** --- SHUTDOWN ABORTED ---
***

R1#
```

3. Les ACL basées sur le contexte (ACL CBAC)

Les ACL *CBAC* offrent la possibilité de distinguer dans un flot de paquets ceux qui appartiennent à une session en cours de ceux qui viennent se heurter aux parois du routeur et n'appartiennent pas à une session valide. Le routeur est alors transformé en un véritable firewall à conservation d'état (en anglais : stateful). Il n'est ainsi plus nécessaire de configurer une ACL dédiée au trafic retour. De plus, il devient possible de laisser le routeur prendre l'initiative d'ouvrir des ports à la volée en fonction de la négociation protocolaire de certaines applications multimédias. Le déploiement de telles ACL aide à combattre les attaques de déni de service par saturation de la pile TCP/IP. Les ACL *CBAC* ont aussi la capacité d'inspecter les commandes passées dans les protocoles filtrés à la recherche d'attaques parmi les plus connues. Les ACL *CBAC* nécessitent la version firewall de l'IOS.

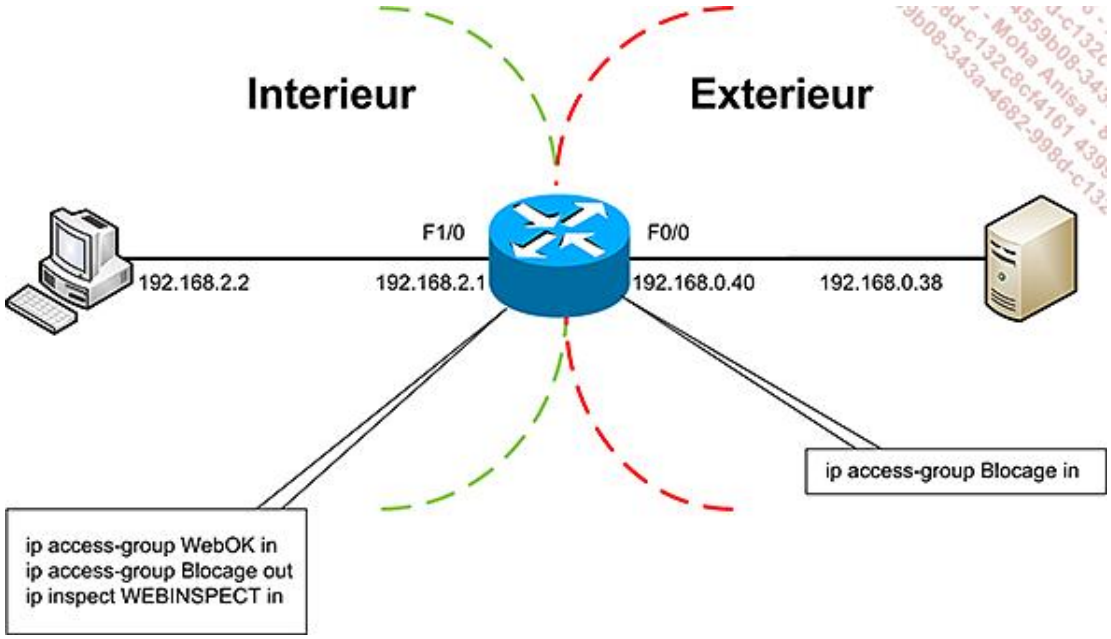
Résumons-en les possibilités :

- Ouverture dynamique de règles autorisant le retour d'un trafic ayant débuté dans une zone de confiance.
- Inspection protocolaire.
- Surveillance des numéros de séquence TCP
- Paramétrage de l'expiration des sessions.
- Dispositif d'alerte.
- Blocage des trafics suspects.
- Blocage d'applets Java.
- Filtrage d'URL

© ENI Editions - All rigths reserved - Moha Anisa

Les ACL CBAC sont particulièrement indiquées pour améliorer la sécurité des architectures voix sur IP. Cisco a développé son propre protocole voix qui porte le nom de *skinny* ou SCCP. Les téléphones IP sont dépendants d'un serveur central (le Call Manager) auquel ils sont connectés et avec qui ils échangent des messages de maintien (keepalive). Lors de l'établissement d'une communication avec un autre poste IP, le Call Manager désigne à l'appareil appelant l'adresse IP de son correspondant ainsi qu'un port. Si on considère plusieurs communications réparties sur un réseau étendu, il faudrait procéder à l'ouverture d'autant de ports sur les équipements de sécurité que sont les firewall. Ici interviennent les ACL CBAC qui ouvrent (et ferment) à la demande les ports nécessaires à l'établissement des communications. Notons que les ACL CBAC ajoutent à la fonction que nous venons de décrire la technologie d'inspection applicative que nous retrouvons dans les fonctions de détection d'intrusion de l'IOS firewall. Dans le cas de la voix sur IP, les en-têtes du protocole SCCP sont inspectés à la recherche d'une incohérence pouvant masquer une attaque.

Examinons à présent une implémentation unidirectionnelle des ACL CBAC. Cet exemple est simplifié afin de ne pas nuire à l'explication. Sachez toutefois qu'une seule ACL CBAC peut examiner plusieurs protocoles et que les ACL CBAC sont positionnables dans toutes les directions.



Nous observons sur ce schéma un PC connecté à un routeur lui-même relié à un serveur. L'objectif à atteindre ici est d'ouvrir dynamiquement l'ACL *Blocage* positionnée sur l'interface extérieure (f0/0) afin de laisser entrer le trafic retour issu des requêtes lancées par le PC vers le serveur. Tout autre trafic entrant sera bloqué.

```
ip inspect max-incomplete low 50
ip inspect max-incomplete high 100
ip inspect one-minute low 50
ip inspect one-minute high 100
ip inspect name WEBINSPECT http alert on audit-trail on
```

Nous appliquons tout d'abord quelques commandes afin de nous prémunir contre les attaques par déni de service qui consistent à ouvrir des connexions TCP à moitié et à les laisser dans cet état. Les commandes `ip inspect max-incomplete high 100` et `ip inspect max-incomplete low 50` sont complémentaires. Il s'agit ici de demander au routeur d'éliminer les connexions (à moitiés ouvertes) lorsque leur nombre dépasse cent et d'arrêter de les supprimer lorsqu'il n'en reste que 50. Les deux commandes suivantes `ip inspect one-minute low` et `ip inspect one-minute high` sont similaires mais se basent sur le nombre de connexions (à moitié ouvertes) par minute.

Puis vient la commande `ip inspect name WEBINSPECT http` qui introduit la liste des protocoles à inspecter. Ici, nous inspectons le protocole http et nous activons les alertes et le suivi des évènements. Ces informations seront à dessein dirigées vers un serveur de type *syslog*.

```
Interface FastEthernet0/0
 description EXTERNE
 ip address 192.168.0.40 255.255.255.0
 ip access-group blocage in
!
interface FastEthernet1/0
 description INTERNE
 ip address 192.168.2.1 255.255.255.0
 ip access-group WebOK in
 ip inspect WEBINSPECT in
!
```

© ENI Editions - All rigths reserved - Moha Anisa

```
ip access-list extended Blocage
 deny   ip any any
ip access-list extended WebOK
 permit tcp any any eq www
!
```

Sur l'interface externe du routeur nous trouvons une ACL nommée *Blocage* et appliquée au trafic entrant comme l'indique le mot `in`. Cette ACL dans le cas présent interdit tout trafic entrant sur l'interface externe. C'est sur cette ACL que les paquets de retour seront pourtant bel et bien autorisés à pénétrer vers l'intérieur du réseau à condition qu'ils aient satisfait les exigences de l'inspection. Ces ouvertures sont dynamiques et commandées par l'inspection directement sur l'ACL.

Sur l'interface interne nous trouvons une ACL (appliquée au trafic entrant) qui autorise n'importe quelle station à communiquer vers n'importe quel serveur en http et la commande `ip inspect WEBINSPECT in` qui déclenche le processus d'inspection. Il est important de noter que cette dernière ACL est indispensable au bon fonctionnement de CBAC. Il est obligatoire d'autoriser le trafic par le biais d'une ACL afin qu'il soit pris en compte par l'inspection.

```
FW#sh ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [50 : 100] connections
max-incomplete sessions thresholds are [50 : 100]
max-incomplete tcp connections per host is unlimited. Block-time 0
minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name WEBINSPECT
    http alert is on audit-trail is on timeout 3600

Interface Configuration
 Interface FastEthernet1/0
  Inbound inspection rule is WEBINSPECT
    http alert is on audit-trail is on timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is WebOK

Established Sessions
 Session 64AAAF84 (192.168.2.2:55046)=>(192.168.0.38:80) http
SIS_OPEN
```

Nous proposons ici pour mémoire le résultat de la commande `show ip inspect all` qui retourne un résumé de la mise en œuvre de la technique CBAC. Notons qu'une session est en cours entre la machine du réseau interne et le serveur http situé à l'extérieur. La session est identifiée par un numéro d'ordre et mentionne le quadruplet à la base de toute communication TCP/IP.

```
FW#sh ip inspect stat
Packet inspection statistics [process switch:fast switch]
  tcp packets: [3:15781]
  http packets: [0:9937]
Interfaces configured for inspection 1
Session creations since subsystem startup or last reset 3
Current session counts (estab/half-open/terminating) [1:0:0]
Maxever session counts (estab/half-open/terminating) [1:1:1]
Last session created 00:05:17
Last statistic reset never
Last session creation rate 0
Maxever session creation rate 1
Last half-open session total 0
```

Ici, nous observons les statistiques de l'inspection.

Les lignes `Current session counts` et `Maxever session counts` indiquent respectivement le nombre de sessions (établies, semi-ouvertes et se terminant) pour l'instant considéré (current) et le maximum compté depuis la mise en service de l'ACL.

```
IP: tableid=0, s=192.168.2.2 (FastEthernet1/0), d=192.168.0.38
(FastEthernet0/0), routed via FIB
```


© ENI Editions - All rigths reserved - Moha Anisa

```
*Mar  1 02:34:57.907: %FW-6-SESS_AUDIT_TRAIL_START: Start http
session: initiator (192.168.2.2:36663) -- responder
(192.168.0.38:80)

*Mar  1 02:34:57.915: IP: s=192.168.2.2 (FastEthernet1/0),
d=192.168.0.38 (FastEthernet0/0), g=192.168.0.38, len 60, forward

*Mar  1 02:34:57.919:     TCP src=36663, dst=80, seq=4135566562,
ack=0, win=5840 SYN

*Mar  1 02:35:03.155: %FW-6-SESS_AUDIT_TRAIL: Stop http session:
initiator (192.168.2.2:36663) sent 432 bytes -- responder
(192.168.0.38:80) sent 257 bytes

*Mar  1 02:35:09.475: IP: s=192.168.94.1 (FastEthernet1/0),
d=239.255.255.250, len 312, access denied
```

Sur cette capture de la commande `debug ip packet detail` et de la console, nous observons derrière le signe %FW-6 l'interception du trafic par l'ACL CBAC et toujours le quadruplet.

```
FW#sh ip access-lists
Extended IP access list Blocage
    10 deny ip any any (504 matches)
Extended IP access list WebOK
    10 permit tcp any any eq www (15258 matches)
```

Les compteurs des ACL nous montrent que du trafic entrant a été bloqué (en entrée) sur l'interface externe.

```
IP: tableid=0, s=192.168.0.38 (FastEthernet0/0), d=192.168.2.2
(FastEthernet1/0), routed via FIB

IP: s=192.168.0.38 (FastEthernet0/0), d=192.168.2.2
(FastEthernet1/0), len 40, access denied

TCP src=80, dst=55046, seq=1764435692, ack=1006152707, win=512 ACK

IP: tableid=0, s=192.168.0.40 (local), d=192.168.0.38
(FastEthernet0/0), routed via FIB

IP: s=192.168.0.40 (local), d=192.168.0.38 (FastEthernet0/0), len
56, sending ICMP type=3, code=13
```

Cet extrait montre le routeur recevant un paquet forgé avec l'utilitaire *HPING2* qui tente de s'introduire au travers de l'ACL *CBAC* en se présentant comme un trafic retour. À cet effet nous avons retourné les adresses source et destination ainsi que les ports source et destination et nous avons ajouté le drapeau *ACK*. Le routeur refuse le paquet et envoie vers la machine tentant d'usurper la connexion un message ICMP type 3 (destination injoignable) code 13 (communication interdite administrativement).

Pour conclure cette partie de chapitre sur les ACL, voici une indication sur leur emplacement idéal. Les ACL sont idéalement positionnées au plus près des éléments à protéger nous y reviendrons au cours du chapitre sur l'architecture générique de la sécurité des réseaux. Prenons trois exemples :

- La protection d'un réseau par rapport à Internet s'effectue logiquement à l'entrée du réseau et plus particulièrement sur le routeur d'accès.
- La protection d'une ferme de serveur s'effectue à l'entrée du *VLAN* qui héberge les ressources.
- Le filtrage sur un *VLAN* utilisateurs est effectué afin de déterminer si les adresses sources qui tentent de sortir du *VLAN* sont dans les plages d'adressages convenues. Ce filtrage est mis en place en sortie du *VLAN* avant la connexion au reste du réseau.

© ENI Editions - All rigths reserved - Moha Anisa

IPSec

L'objectif est d'assurer la confidentialité et l'authenticité des données en transit sur un réseau non sécurisé.

On a beaucoup écrit sur la cryptographie et elle est toujours l'objet de nombreux fantasmes. La cryptographie intrigue toujours. Est-elle l'apanage des services secrets ? Que protège-t-elle vraiment ? Qui en est le maître absolu ? La cryptographie protège vos secrets et vous en êtes le maître absolu. Ni plus, ni moins. L'art de dissimuler une information remonte aux sources de l'humanité. Depuis les temps les plus anciens, les civilisations en guerre ont toujours souhaité protéger les secrets militaires tactiques. Simples permutations de lettres ou enroulements de lanières de cuir sur des cylindres de bois au diamètre secret, la cryptographie a lentement évolué pour bénéficier depuis le 19^{e} siècle des recherches les plus poussées en mathématiques. Rendons ici un modeste hommage à Pierre de Fermat dont le théorème dit « du petit Fermat » servit de base de travail aux trois mathématiciens américains Rivest, Shamir et Adleman (RSA) qui découvrirent l'un des systèmes de chiffrement qui figure parmi les plus utilisés dans le monde. Nous n'allons pas ici entrer dans les détails tortueux mais ô combien passionnants du calcul modulaire mais débuter cette approche de la cryptographie sur les équipements Cisco par quelques règles d'or :

- La force d'un système de chiffrement repose avant tout sur la force de la clé plutôt que sur la technologie sous jacente (bien qu'elle ait son importance). À titre d'exemple le système dit du chiffre de Vernam nécessite une feuille de papier, un bon crayon et... un roman de votre choix. Ce chiffre manuel est reconnu par les plus grands spécialistes comme le système le plus sûr car la clé de chiffrement est aussi longue que le texte à chiffrer. Les amateurs de cinéma se remémoreront sans peine une scène du film "l'armée des ombres" montrant Lino Ventura en train de chiffrer un message à l'aide d'un livre dont son correspondant possède la même édition.

- Les fondements sécurité d'un système de chiffrement reposent sur la protection dont bénéficient les clés. Cette remarque parait incongrue de prime abord mais, certaines sociétés n'hésitent pas pour des raisons de commodité à confier leurs clés à des tiers. Quel crédit apporter à ce genre de pratiques ?

Il existe deux techniques d'emploi du chiffrement qui sont le chiffrement en ligne et le chiffrement hors ligne :

- Le chiffrement en ligne chiffre les informations lors de leur transmission. IPSec entre dans cette catégorie.

- Le chiffrement hors ligne nécessite un chiffrement de l'information avant de la transmettre car l'équipement de transmission ne possède aucune fonction cryptographique. Le chiffre de Vernam dans sa version manuelle entre dans cette catégorie.

Il existe deux types de clés pour le chiffrement :

- Les clés symétriques. La même clé est utilisée par les correspondants pour le chiffrement et le déchiffrement. Ce type de clé est utilisé par IPSec.

- Les clés asymétriques. Chaque correspondant possède un couple de clés, l'une sert au chiffrement, l'autre au déchiffrement. Nous ne traiterons pas cette technique. Sachez toutefois qu'elle est employée pour la signature électronique.

IPSec est un ensemble de protocoles qui permet un chiffrement en ligne de l'information, le protocole est directement implémenté sur les routeurs, les clés sont de type symétrique. IPSec est composé :

- Du protocole IKE (*Internet Key Exchange*) qui sert à :
    - Authentifier les deux partenaires.
    - Négocier les paramètres de chiffrement
    - Protéger la suite des échanges dont l'échange des clés de session.
- De deux modes (au choix) qui permettent soit de transmettre les paquets en conservant les adresses sources et destinations d'origine soit de générer des paquets ayant comme adresses source et destination les interfaces externes des routeurs.
- De deux modes (au choix) permettant soit l'authentification seule des paquets, soit le chiffrement et l'authentification des paquets.

Examinons ces trois étapes dans le cadre d'un chiffrement entre deux routeurs.

© ENI Editions - All rigths reserved - Moha Anisa

La mise en œuvre de IKE se déroule en deux phases :

- La première phase permet aux routeurs de s'authentifier mutuellement et de monter un canal sécurisé afin de procéder à la seconde phase. L'authentification mutuelle s'effectue par le biais d'une paires de clés pré partagées (*Pre Shared Key*) ou sur présentation de certificats. Un échange de messages permet grâce au protocole *Diffie-Hellman* de calculer un secret commun qui permet à son tour de calculer les futures clés de session.

- La seconde phase est entièrement protégée et scelle véritablement l'association entre les deux partenaires IPSec. Les clés de sessions sont calculées et les paramètres de renégociation fixés.

À l'issue de cette négociation le tunnel proprement dit est établi conformément aux choix fixés dans la configuration. Ces choix permettent comme nous l'avons décrit brièvement plus haut :

- En ce qui concerne le mode de transmission :

  - De conserver les adresses sources et destination d'origine. C'est le mode transport.

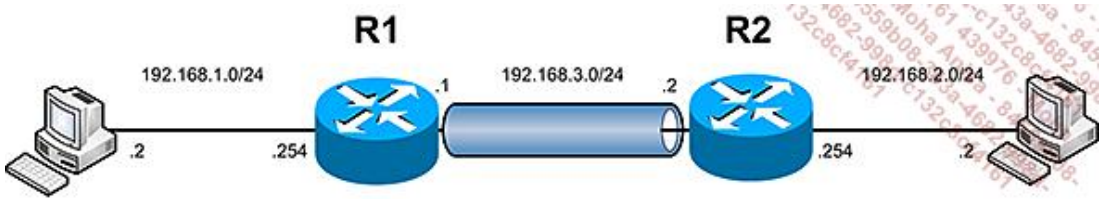
  - De chiffrer les adresses d'origine (c'est-à-dire tout le paquet original) et de doter le nouveau paquet ainsi obtenu de nouvelles adresses qui correspondent aux adresses des interfaces externes des routeurs. C'est le mode tunnel.

- En ce qui concerne la protection des paquets :

  - D'authentifier le paquet et de garantir son intégrité sans le chiffrer. C'est le mode *AH* (*Authentication Header*).

  - De chiffrer, d'authentifier et de garantir l'intégrité des paquets. C'est le mode *ESP* (*Encryption Security Payload*).

Il est à présent temps d'examiner une configuration.



Voici comme de coutume une configuration très simple. Nous n'abordons pas la traduction d'adresse qui serait nécessaire si le réseau central était public. Cette configuration utilise une paire de clés pré-partagée pour la phase d'authentification mutuelle des routeurs. Étudions les étapes de configuration du routeur R1. Ici les communications sont chiffrées entre les deux interfaces des routeurs R1 et R2 qui se font face.

```
R1(config)#ip access-list extended CHIFFRER
R1(config-ext-nacl)#10 permit ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255
```

Avant toute chose, une ACL est définie afin d'identifier le trafic à chiffrer, nous avons évoqué cet aspect des ACL qui n'ont pas pour vocation unique le filtrage des paquets à des fins de blocage.

```
R1(config)#key config-key password-encrypt securitemaximale123
R1(config)#password encryption aes
```

Cette commande permet de chiffrer en AES les clés pré-partagées dans la configuration du routeur.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr aes
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
```

Nous observons ici la configuration des phases du protocole *IKE* qui est appelé ISAKMP. Le routeur est configuré avec une stratégie (`policy`) unique pour des raisons de clarté. Sachez qu'il est envisageable de configurer plusieurs stratégies `policy` ainsi que des profils. Les phases d'authentification mutuelle des routeurs sont protégées avec le

© ENI Editions - All rigths reserved - Moha Anisa

protocole *AES* et le protocole de *Diffie-Hellman* au niveau 5 (`group 5`), les deux routeurs utilisent une même clé pré-partagée. Comme nous l'avons souligné précédemment, il est indispensable de protéger les échanges d'authentification mutuels afin de se prémunir contre toute tentative d'intrusion lors de cette phase.

```
R1(config)#crypto isakmp key 0 cisco address 192.168.3.2
```

Voici la clé pré-partagée commune aux deux routeurs. Sur le routeur R1, nous configurons la clé qui correspond au partenaire IPSec. C'est pourquoi figure sur cette ligne de commande l'adresse IP du routeur R2. La clé est en clair dans cette ligne de commande. Une clé pré-partagée est acceptée jusqu'à 128 caractères. Ici, la clé est le mot CISCO. Notons au passage qu'il est recommandé de ne jamais utiliser une clé aussi triviale. Référez-vous en la matière aux recommandations de sécurité des mots de passe (utilisation de caractères spéciaux, de chiffres, de majuscules). Si nous passons en revue la configuration nous trouvons la clé sous cette forme :

```
crypto isakmp key 6 A_gL\QY[FDAXg_DOFi[AKY^P\SSAAB address
192.168.3.2
```

La clé est ici chiffrée avec le protocole AES. Nous remarquons le chiffre 6 entre le mot *key* et la clé au lieu du chiffre 0. Cela confirme le chiffrement de la clé.

```
R1(config)#crypto ipsec security-association lifetime kilobytes
3000
R1(config)#crypto ipsec security-association idle-time 900
```

Les deux commandes `security-association lifetime` et `idle-time` limitent dans le temps et en volume la validité de l'association des deux routeurs. Au-delà de la limite de 3 mégaoctets ou de 900 secondes sans échange, les clés de chiffrement sont renégociées.

```
R1(config)#crypto ipsec transform-set CHIFFRE esp-aes 256 esp-sha-
hmac
```

Nous choisissons de chiffrer les paquets avec le protocole `aes-256` et d'en protéger l'intégrité avec le protocole de hachage `sha`, par défaut le mode tunnel est employé cela signifie que les paquets d'origine (et notamment les adresses IP) seront chiffrés masquant ainsi leur origine et leur destination sur les réseaux locaux.

```
R1(config)#crypto map LAN-LAN_VPAN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
```

Voici la commande qui nomme la fonction IPSec et qui la rattache à la stratégie `policy` créée au début. Le routeur nous informe que cette commande n'est d'aucune utilité tant qu'un partenaire IPSec ne sera pas déclaré et tant qu'une ACL déterminant le trafic à chiffrer n'aura pas été créée. Poursuivons avec les sous-commandes de `crypto map`.

```
R1(config-crypto-map)#set peer 192.168.3.2
R1(config-crypto-map)#set transform-set CHIFFRE
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#match address CHIFFRER
```

Détaillons cette séquence de commandes.

Tout d'abord le partenaire IPSec est déclaré. Il s'agit de l'adresse externe du routeur R2. Puis, nous appelons les fonctions de chiffrement définies auparavant avec la commande `crypto ipsec transform-set`. La commande suivante est importante, elle permet de sécuriser les messages chiffrés avec les clés antérieures à une clé compromise grâce à une renégociation par le protocole de *Diffie-Hellman* (avec un modulo élevé). En clair, si une clé venait à être compromise, un attaquant aurait du mal à déchiffrer les messages émis avec les clés précédentes, car ces dernières ne seraient plus liées entre elles. Enfin, l'ACL nommée CHIFFRER est appelée. Cette dernière, définit le trafic à chiffrer sur le lien.

```
R1(config)#int f1/0
R1(config-if)#crypto map LAN-LAN_VPAN
```

Comme de coutume avec les routeurs Cisco, tout le travail que nous venons d'effectuer s'applique sur une interface physique ou logique. En l'occurrence, l'interface extérieure du routeur R1 (*FastEthernet 1/0*).

Une configuration digne de ce nom s'achève toujours par quelques commandes `show` afin de la valider.

```
R1#sh crypto engine connections active

ID Interface          IP-Address   State Algorithm   Encrypt  Decrypt
001 FastEthernet1/0   192.168.3.1  set   AES256+SHA  0        7
2002 FastEthernet1/0  192.168.3.1  set   AES256+SHA  7        0
```

© ENI Editions - All rigths reserved - Moha Anisa

Les deux dernières lignes nous montrent que 7 paquets ont été chiffrés et déchiffrés par le routeur. Notons que le routeur différencie les directions dans lesquelles s'effectuent les opérations (ID 2001 et 2002). Il en est même pour les associations de sécurité lorsque deux routeurs sont partenaires, elles sont aussi au nombre de deux.

```
R1#sh crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: LAN-LAN_VPAN, local addr 192.168.3.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
(192.168.2.0/255.255.255.0/0/0)

   current_peer 192.168.3.2 port 500

     PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. Failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 3, #recv errors 0

     local endpt.: 192.168.3.1, remote crypto endpt.: 192.168.3.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
     current outbound spi: 0xF8CD0F54(4174188372)

     inbound esp sas:
      spi: 0x81CD9180(2177732992)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: LAN-LAN_VPAN
        sa timing: remaining key lifetime (k/sec): (2861/3587)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound esp sas:
      spi: 0xF8CD0F54(4174188372)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: LAN-LAN_VPAN
        sa timing: remaining key lifetime (k/sec): (2861/3579)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
```

Le retour de cette commande a été tronqué pour plus de visibilité. Nous y distinguons clairement des deux associations de sécurité. Nous observons également trois erreurs. Elles correspondent aux premiers paquets qui sont perdus lors de la négociation protocolaire entre les partenaires IPSec.

Nous passons volontairement sous silence le retour des commandes `debug` qui sont d'une très grande utilité mais extrêmement verbeuses pour être reproduites ici, nous vous laissons le soin de les découvrir et d'observer l'établissement d'IPSec. Ces commandes sont : `debug crypto ipsec`, `debug crypto isakmp` et `debug crypto engine`. Pour mémoire, la commande (ultra courte) mettant fin à tous les `debug` et permettant de retrouver un calme relatif sur la console est : `u all` (elle résume la commande `undebug all`).

Il existe deux méthodes d'authentification mutuelle pour IPSec qui sont les clés pré-partagées (que nous venons de décrire) et les certificats. Ces derniers offrent plus de souplesse une fois en place et libèrent l'administrateur des risques inhérents à la gestion des clés sous forme de séquence de caractères. Toutefois, la mise en place et le déploiement d'une infrastructure de certificats (dite PKI) est complexe et ne se justifie en terme de praticité pour la configuration qu'au-delà d'un nombre élevé de routeurs. Ici c'est la politique de sécurité et ses directives en la matière qui prévaudront. Sachez que le niveau de sécurité d'une clé pré-partagée est tout à fait acceptable à condition de respecter quelques règles de base qui sont une production à partir d'un générateur aléatoire sûr et une gestion rigoureuse des clés de la génération à la destruction en passant par la distribution. À titre d'exemple, cette commande du programme openssl génère une clé aléatoire de 128 caractères qui est la taille maximale d'une clé pré-partagée : openssl rand -base64 128.

© ENI Editions - All rigths reserved - Moha Anisa

Les ACL de la configuration IPSec servent à définir le trafic qui est à chiffrer sur le lien. Un trafic non défini par l'ACL passera sur le lien en clair. Il est commun de penser qu'il sera refusé sur l'interface. Il n'en est rien !

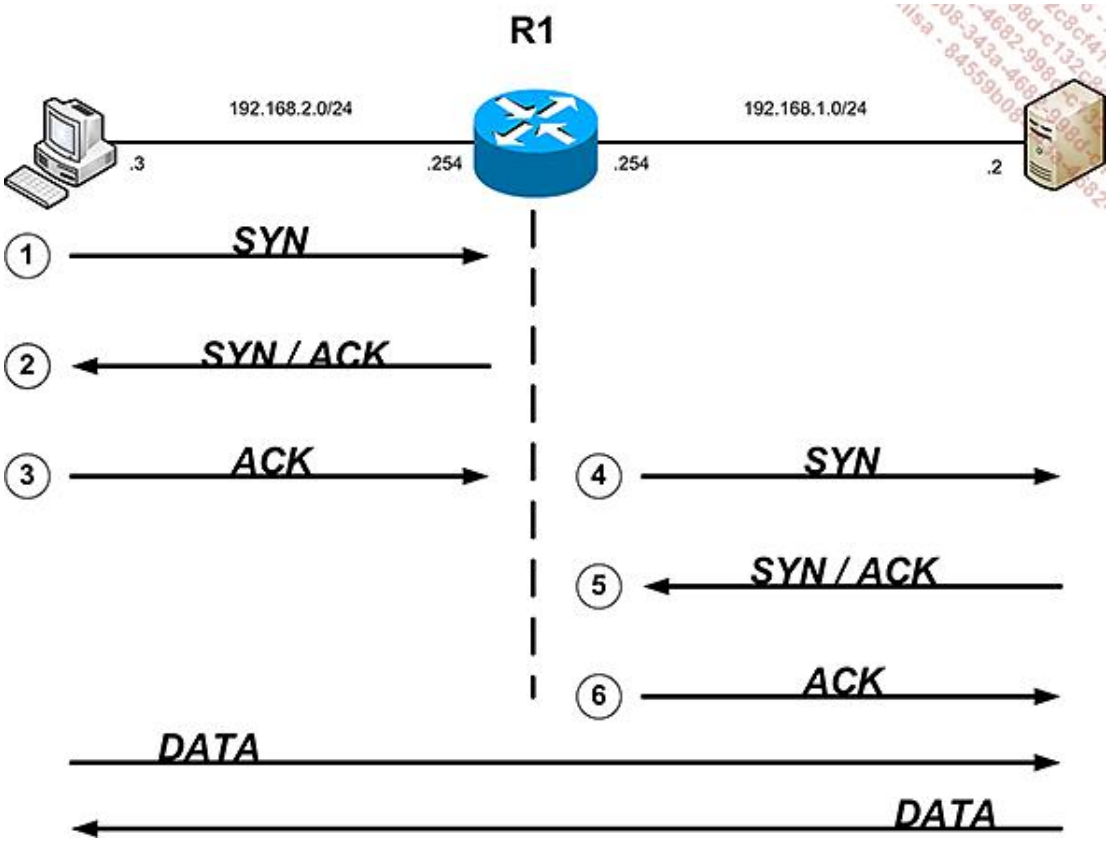
© ENI Editions - All rigths reserved - Moha Anisa

TCP intercept

L'objectif est de se protéger contre les attaques par inondation de paquets SYN autrement appelée *syn flooding*.

Les connexions TCP/IP font appel à un mécanisme bien connu pour l'établissement des communications. Souvent nommée *three way handshake*, cette séquence si elle est mal exécutée peut mobiliser rapidement les ressources d'un serveur par l'allocation de plus en plus de mémoire aux connexions entrantes jugées légitimes. Une attaque consiste à monopoliser les ressources du serveur en lançant vers celui-ci une multitude de paquets d'ouverture de connexions sans toutefois aller jusqu'à la conclusion du *three way handshake*. Cette attaque par déni de service est redoutable.

Les routeurs mettent en œuvre une protection contre cette attaque. Positionné entre un serveur et ses clients potentiels, le routeur valide les demandes de connexions avant de le retransmettre au serveur. Si tel n'est pas le cas, la tentative de connexion est annulée. La durée de la tentative d'établissement de la connexion est étroitement surveillée et des réglages sont disponibles afin de la limiter. La mise en place du dispositif est effective après application d'une ACL qui détermine le quadruplet à surveiller.



Le routeur reçoit dans un premier temps la demande de connexion du client et conclut avec lui le *three way handshake*. Il procède à la même opération vis-à-vis du serveur et se retire laissant les deux partenaires continuer leur échange. Si un client ne répond pas dans le temps imparti ou s'il persiste à envoyer en nombre des paquets de type SYN sans répondre aux sollicitations du routeur, la fonction *tcp intercept* intervient en éliminant les communications à moitié ouvertes au fur et à mesure.

Détaillons la mise en œuvre de cette fonctionnalité en examinant la configuration.

```
R1(config)# ip access-list extended TCP_INTER
R1(config-ext-nacl)#10 permit tcp any host 192.168.1.3 eq www
```

La fonctionnalité *tcp intercept* nécessite tout d'abord une ACL afin de déterminer le trafic à surveiller. Présentement, le trafic désigné est celui à destination du serveur 192.168.1.3 sur le port tcp www (80).

```
R1(config)# ip tcp intercept mode intercept
R1(config)# ip tcp intercept list TCP_INTER
R1(config)# ip tcp intercept one-minute low 50
R1(config)# ip tcp intercept one-minute high 100
```

Ces quatre commandes prises dans l'ordre lancent la fonction *tcp intercept*, donnent la référence de l'ACL puis fixent à 100 connexions incomplètes par minute le seuil haut à partir duquel il faudra commencer à purger pour ne pas justement dépasser ce seuil. Si le nombre de connexions incomplètes passe en dessous de 50 connexions, *tcp intercept* les laisse expirer.

© ENI Editions - All rigths reserved - Moha Anisa

```
R1#sh tcp intercept connections
Incomplete:
Client               Server             State    Create
Timeout    Mode

Established:
Client               Server             State    Create
Timeout    Mode
192.168.2.3:44435    192.168.1.3:80     ESTAB    00:00:05
23:59:55   I
```

Une connexion complète est établie entre le client et le serveur, ici, nous n'observons aucune connexion incomplète.

À partir du client, nous allons avec l'utilitaire `hping2` lancer vers le serveur des demandes de connexions. Il s'agit de paquets avec le drapeau SYN. La commande est : `hping2 192.168.1.3 -p 80 -S`.

```
R1#sh tcp intercept connections
Incomplete:
Client                Server             State     Create
Timeout    Mode
192.168.2.3:2448      192.168.1.3:80     SYNRCVD   00:00:14
00:00:00   I
192.168.2.3:2449      192.168.1.3:80     SYNRCVD   00:00:13
00:00:01   I
192.168.2.3:2450      192.168.1.3:80     SYNRCVD   00:00:12
00:00:02   I
192.168.2.3:2451      192.168.1.3:80     SYNRCVD   00:00:11
00:00:03   I
192.168.2.3:2452      192.168.1.3:80     SYNRCVD   00:00:10
00:00:04   I
192.168.2.3:2453      192.168.1.3:80     SYNRCVD   00:00:09
00:00:05   I

Established:
Client                Server             State     Create
Timeout    Mode
192.168.2.3:41775     192.168.1.3:80     ESTAB     00:00:17
23:59:57   I
```

Voici un extrait des connexions complètes et incomplètes visibles sur le routeur. Notons que l'état mentionne SYNRCVD qui signifie SYN reçu.

```
R1#sh tcp intercept stat
Intercepting new connections using access-list TCP_INTER
99 incomplete, 1 established connections (total 100)
399 connection requests per minute
```

La commande `show` ci-dessus indique le nombre de connexions bloquées et incomplètes (99), montre une connexion établie et le taux de 399 connexions par minutes.

Peu de temps après, le message suivant apparaît sur la console :

```
%TCP-6-INTERCEPT: getting aggressive, count (100/100) 1
```

Ce message issu de *tcp interpect* nous informe que le seuil haut est atteint. Si nous stoppons l'envoi de paquets avec hpihgz le message suivant s'affiche :

```
%TCP-6-INTERCEPT: calming down, count (0/50) 1 min 3n
```

Ici, le routeur indique un retour à une situation normale telle qu'elle a été définie dans la configuration c'est-à-dire 50 connexions par minute.

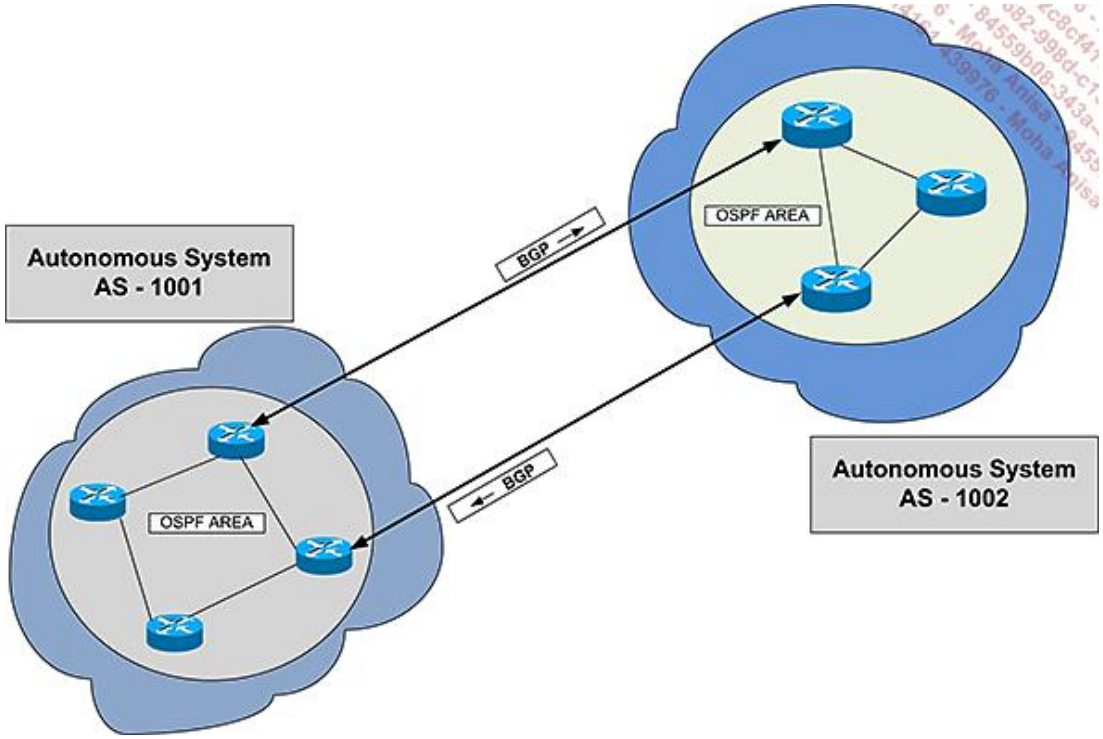
Il est important de prêter une attention toute particulière quant à la définition des valeurs de paramétrage. En effet, un réglage trop bas conduirait sans aucun doute le routeur à écarter du trafic légitime. Une technique consiste à observer le trafic lors d'une activité normale du réseau et tout particulièrement le nombre maximum de connexions ouvertes et à moitiés ouvertes. À partir de ces valeurs, il est recommandé d'appliquer un petit cœfficient de sécurité pour ne pas bloquer le réseau lors d'un pic de trafic légitime.

© ENI Editions - All rigths reserved - Moha Anisa

Les protocoles de routage

L'objectif est de protéger les échanges protocolaires des protocoles de routage afin que le trafic soit correctement acheminé sur le réseau, en entrée et en sortie de celui-ci.

Que l'on considère un réseau dit local, métropolitain ou l'Internet tout entier, aucune communication ne saurait avoir lieu sans l'aide des protocoles de routage. Ils forment avec les services DNS les fondations de nos réseaux actuels. Ces fondations toutefois ne manquent pas de susciter la convoitise des personnes les plus malveillantes. Parmi les protocoles de routage qui nous intéressent plus particulièrement figurent BGP (*Border Gateway Protocol*) et OSPF (*Open Shortest Path First*) car ce sont les plus populaires. Ces deux protocoles sont disponibles sur la plupart des équipements de routage quel que soit le constructeur. Si OSPF est majoritairement déployé sur les réseaux privés, BGP est pour sa part le protocole de routage d'Internet.



Voici à l'œuvre les deux protocoles de routage. Les deux systèmes autonomes (AS - 1001 et AS - 1002) sont deux entités indépendantes l'une de l'autre et possédant chacune son propre protocole de routage. Les deux AS utilisent pour la gestion de leurs routes le protocole OSPF indépendamment l'une de l'autre. Si une connexion est envisagée entre les deux AS, il faut mettre en place un protocole de routage différent d'OSPF afin de garantir à chaque AS une indépendance totale pour la gestion de ses routes tout en communiquant certaines d'entres-elles avec son partenaire. C'est ici qu'intervient le protocole BGP dans son rôle de transporteur de routes entre systèmes autonomes. Cette explication constitue une approche (rapide et schématique il est vrai) du réseau Internet. Cette vue nous montre aussi l'importance des protocoles de routage. Il est aisé de constater qu'une panne sur l'un ou l'autre des protocoles (et ce malgré les redondances non représentées ici) entrainerait des perturbations dans l'acheminement du trafic. De ces perturbations potentielles vont découler nos exigences de sécurité :

- Résister aux tentatives de déni de service sur le protocole.
- Résister aux tentatives de détournement d'information de routage.

Ces deux exigences générales sont déclinées en mesures de protection qui ne sont pas toutes hélas proposées par le protocole lui-même. En fait, les deux protocoles de routage que nous venons d'évoquer n'embarquent pour leur sécurité qu'un contrôle basé sur un mot de passe et (ou) la fonction de hachage MD5. Cela peut paraître bien mince au regard des menaces qui planent sur les réseaux informatiques mais, dans le domaine des protocoles de routage, les coupures de service les plus sévères ont eu lieu suite à des erreurs de configuration ce qui n'a pas orienté semble-t-il la communauté vers une approche sécuritaire.

Les tentatives de déni de service sur le protocole visent à perturber ce dernier sur ses fonctions dans le but de le perturber, de le ralentir ou de l'arrêter totalement. Les protocoles de routage procèdent à l'échange de messages pour associer entre eux les routeurs d'un même domaine et bien entendu échanger des informations sur les routes disponibles. À titre d'exemple, le protocole OSPF s'il reçoit des messages forgés et contenant des informations erronées aura tendance à utiliser de plus en plus de mémoire lors de ses tentatives de calcul pour réorganiser la topologie du réseau, le tout pouvant également consommer d'importantes quantités de bande passante. Le protocole BGP quant à lui, possède une fonction qui élimine l'information concernant une route si celle-ci tend à apparaitre et à disparaître trop

© ENI Editions - All rigths reserved - Moha Anisa

souvent. Ici aussi, une séquence de messages savamment construits leurrera le routeur et causeront la disparition d'informations de routage. Citons également les attaques par saturation de la bande passante des liens sur lesquels circule un protocole de routage.

Les tentatives de détournement de routage consistent à fournir au protocole de routage des informations de routage erronées en vue de détourner le trafic vers un endroit précis ou pire, de faire disparaitre des routes.

Quels sont les moyens mis à notre disposition pour contrecarrer efficacement les cas que nous venons de citer ?

Une solution est l'utilisation de la fonction de hachage MD5 qui est disponible pour les deux protocoles. En voici le fonctionnement.

1. La mise à jour de routage et une clé partagée entrent dans une fonction MD5. Un résultat est calculé.

2. La mise à jour de routage et le résultat de la fonction MD5 précédemment calculée sont envoyés aux routeurs destinataires de la mise à jour.

3. Après réception, la mise à jour reçue est de nouveau avec la clé partagée entrée dans la fonction MD5, un résultat est calculé.

4. Ce résultat est comparé à celui reçu avec la mise à jour reçue à l'étape 3.

Ce système est peu coûteux en ressources. Une autre recommandation est de protéger la configuration du routeur contre tout accès illégitime pour que la clé ne tombe pas entre de mauvaises mains.

Pour illustrer cette fonctionnalité, nous avons connecté deux routeurs (R1 et R2) via leurs interfaces réseau respectives afin d'observer leur comportement lors de la mise en œuvre de la protection.

```
R1(config-if)#ip ospf message-digest-key 1 md5 cisco
R1(config-if)#ip ospf authentication message-digest
```

En mode configuration de l'interface, ces deux commandes activent l'authentification telle que décrite.

Le chiffre 1, sur la première commande indique qu'il est possible d'entrer plusieurs clés. Ceci est très utile lors d'un changement des clés sans altérer le fonctionnement du réseau.

```
R1#sh ip ospf interface f1/0
FastEthernet1/0 is up, line protocol is up
  Internet Address 192.168.0.2/24, Area 0
  Process ID 1, Router ID 192.168.0.2, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.0.2, Interface address 192.168.0.2
  Backup Designated router (ID) 192.168.0.1, Interface address
192.168.0.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.0.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 2
    Rollover in progress, 1 neighbor(s) using the old key(s):
      key id 1
```

Ici, nous observons le résultat de la commande `sh ip ospf interface f1/0`. Elle est très utile et montre précisément qu'une mise à jour de la clé est en cours sur le routeur R1 et que le routeur R2 utilise encore l'ancienne clé. Pour effectuer le changement définitif, il suffira sur R2 d'entrer la nouvelle clé et de retirer les anciennes clés des deux routeurs.

```
interface FastEthernet1/0
 ip address 192.168.0.2 255.255.255.0
 ip ospf authentication message-digest
 ip ospf message-digest-key 2 md5 7 104D000A0602
 duplex auto
```


© ENI Editions - All rigths reserved - Moha Anisa

```
 speed auto
```

Si le service de chiffrement des mots de passe (*service password encryption*) est activé, nous notons que la protection du mot de passe dans la configuration du routeur est hélas confiée avec le mode 7 qui est un chiffrement faible. Il faudra donc veiller à bien protéger l'accès au routeur. Quoi qu'il en soit, l'authentification mutuelle des partenaires OSPF (on parle aussi de voisins) est fortement recommandée pour éviter l'introduction d'un routeur étranger au réseau et l'injection d'informations de routage indésirables.

Une autre solution passe par un renforcement de la configuration et l'utilisation d'ACL qui viennent une fois encore au secours de l'administrateur réseau.

Examinons le protocole BGP.

```
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 26001
 neighbor 10.0.0.1 password 7 070C285F4D06
 no auto-summary
```

BGP offre une protection similaire comme le montre la capture ci-dessus. BGP mériterait une protection renforcée tout du moins pour sa version sur IPV4 car il constitue l'épine dorsale d'Internet et aussi de nombreux réseaux d'entreprise étendus. BGP a été conçu à une époque où la sécurité n'était pas la principale des préoccupations car aucune menace sérieuse ne planait encore sur le réseau des réseaux. Le retard a fort heureusement été rattrapé dans la version de BGP destinée à IPV6.

La sécurité des protocoles de routage repose principalement sur la configuration des routeurs et la protection de celle-ci. C'est ici qu'interviennent les ACL. Les principes de base sont simples :

- Identifier les partenaires qui envoient les mises à jour de routage et authentifier ces dernières. BGP qui utilise des communications sur un port TCP bien connu (179) est apte à transiter directement dans un tunnel chiffré. Cette solution impliquerait un déploiement d'IPSec entre routeurs ce qui n'est pas toujours réalisable principalement pour des problèmes de logistique comme la distribution des clés ou des certificats entre des milliers de partenaires n'appartenant pas aux mêmes organisations. Dans le cas d'OSPF, la solution requiert la création d'une interface de type tunnel et son chiffrement avant d'y faire transiter les mises à jour.

- Ne pas accepter d'un de nos partenaires qu'ils nous informent sur nos propres routes internes afin de ne pas créer de boucles de routage. Cette règle est valable dans les deux sens dans la mesure où un routeur partenaire n'est pas non plus intéressé par un retour des mises à jour qu'il envoie.

- Les partenaires étant généralement directement connectés, ne pas accepter de mise à jour venant d'un routeur éloigné. Ceci est réalisable en contraignant les paquets contenant des mises à jour à se présenter avec un TTL (*Time To Live*) supérieur à une certaine valeur que ne pourront jamais posséder des machines lointaines.

- Refuser systématiquement les réseaux dont les préfixes sont réservés par les instances dirigeantes d'Internet. Cette liste qui porte le nom de *bogon networks* est largement diffusée. Il suffit d'associer ces réseaux à une ACL en entrée.

- Ne laisser entrer les mises à jour de routage qu'en provenance de routeurs connus grâce à des ACL étendues.

La liste des réseaux non attribués sur Internet est disponible à l'adresse suivante : http://www.iana.org/assignments/ipv4-address-space

© ENI Editions - All rigths reserved - Moha Anisa

RFC 1918

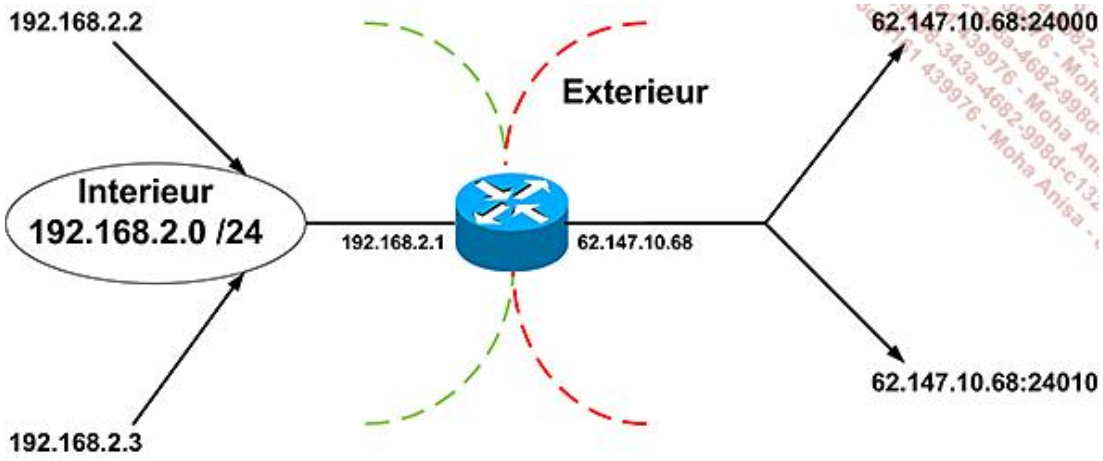
Rares sont les entreprises qui mettent à disposition du public des services Internet nécessitant de grandes quantités d'adresses IP de type 4. Ces dernières années, les adresses IP sont devenues une denrée rare et les entreprises sur leurs réseaux privés en sont de grandes consommatrices.

Afin de palier à un manque global d'adresses IP, il a été décidé au niveau des instances régulatrices d'Internet de proposer aux entreprises trois plages d'adresses IP libres d'utilisation sur les réseaux privés et de fait non valables sur Internet. La mise à disposition d'un mécanisme de conversion entre les adresses privées et les adresses publiques permet toujours aux entreprises de converser avec le monde extérieur. Ce mécanisme porte le nom de NAT (*Network Address Translation*). Avec ce système, les hôtes d'un réseau privé désirant se connecter à Internet le font en utilisant une adresse publique unique et continuent à communiquer entre eux grâce aux adresses réservées. En revanche, un hôte désirant être visible sur Internet doit impérativement disposer d'une adresse publique.

Les plages d'adresses privées, libres d'utilisation et non valables sur Internet sont :

- le préfixe 10.0.0.0 /8 qui représente les adresses IP de 10.0.0.1 à 10.255.255.254 ;
- le préfixe 172.16.0.0 /12 qui représente les adresses IP de 172.16.0.1 à 172.31.255.254 ;
- le préfixe 192.168.0.0 /16 qui représente les adresses IP de 192.168.0.1 à 192.168.255.254.

Les mécanismes de NAT sont généralement effectués par les routeurs ou les pare-feu à la limite entre le réseau privé et Internet.



Nous observons sur ce schéma deux hôtes du réseau privé 192.168.2.0 /24 qui envoient du trafic vers l'extérieur en direction d'Internet. La fonction de traduction d'adresse (NAT) sur le routeur transforme les champs adresses source des paquets sortant et substitue aux adresses privées l'adresse publique de son interface externe. La différenciation entre les deux trafics lors du retour est effectuée grâce au port TCP (ou UDP). Dans notre exemple, les paquets revenant vers le routeur avec un port TCP destination de 24000 seront dirigés vers l'hôte 192.168.2.2.

© ENI Editions - All rigths reserved - Moha Anisa

Conclusion

Au cours de ce chapitre, nous avons examiné les menaces qui pèsent sur cette couche et les mesures de protection adéquates.

La couche 3 du modèle OSI est l'épine dorsale de la majeure partie des réseaux d'entreprise et d'Internet. À ce titre sa sécurité requiert une attention particulière. Si aucune mesure de filtrage n'est appliquée entre les réseaux, les protocoles de routage et les tables éponymes se chargent tout naturellement d'acheminer le trafic tous azimuts. Ce n'est généralement pas l'objectif des réseaux d'entreprise pour lesquels un minimum d'isolation est requis. Pour satisfaire aux exigences de filtrage, les listes de contrôles d'accès (ACL) sont d'un grand secours pour pratiquer toutes sortes de restrictions de trafic. Les ACL de type *CBAC* sont en mesure de transformer un routeur en pare-feu à conservation d'état (*stateful*). Ce type d'équipement conserve en mémoire les connexions sortantes afin d'autoriser dynamiquement le trafic retour.

IPSec qui est composé d'une suite de protocoles a la faveur des entreprises pour le chiffrement en ligne des données sur des circuits de type point à point ou point à multipoints. Son utilisation toutefois semble en perte de vitesse dans le domaine des connexions nomades car son implémentation et sa configuration bien que souples restent assez délicates.

Les protocoles IP et TCP sont très liés. À ce titre, nous avons abordé les mesures de sécurité qui visent à protéger la pile IP contre les attaques par déni de service qui saturent les services en demandes de connexions laissées sans suite. Il convient de prendre en compte ce type de menaces car la saturation d'un réseau conduit rapidement à son effondrement avec les conséquences que cela implique.

L'acheminement des paquets à bon port est déterminant pour le bon fonctionnement d'un réseau. Il s'agit là d'une évidence. Les protocoles de routage dynamiques qui ont remplacé les tables statiques méritent pour leur configuration une attention particulière car, bien qu'ils soient vulnérables à des attaques ayant pour but de dérouter le trafic, les protocoles de routage sont aussi victimes d'erreurs de configuration. L'authentification des mises à jour s'avère alors indispensable.

© ENI Editions - All rigths reserved - Moha Anisa

Généralités

Ces quatre lettres font partie de notre environnement quotidien : Wi-Fi. Chez soi, au restaurant, dans les gares et les aéroports, les points d'accès ont ces dernières années colonisés les lieux publics et les salons. Facile d'accès et peu coûteux, parfois gratuit pour le grand public, le *Wi-Fi* supplante peu à peu les réseaux câblés dans les entreprises et apporte bien sûr son lot de soucis liés à la sécurité. Le *Wi-Fi* fait appel aux ondes radios qui par nature ne connaissent comme limite que leur portée et sa sécurité a connu dès ses débuts de graves déboires avec le protocole WEP dont on connait à présent les faiblesses.

Parmi les utilisations des réseaux sans fil de type *Wi-Fi* on trouve :

- Le remplacement des lignes louées entre des bâtiments se trouvant de part et d'autre d'un domaine public. Les équipements Wi-Fi (généralement des ponts) sont dans ce cas connecté à des antennes directionnelles qui se font face à des distances pouvant atteindre plusieurs dizaines de mètre.
- Les connexions au réseau local itinérantes qui n'utilisent plus de câblage standard (connecteur RJ45).
- Les connexions à Internet libres (ou pas) pour des populations itinérantes à partir de lieux publics ou privés.

Les réseaux Wi-Fi se composent principalement, de clients radio, de bornes d'accès (ou points d'accès) et de manière optionnelle d'une infrastructure de sécurité externe.

Les clients radios sont l'équivalent des cartes réseaux Ethernet telles que nous les connaissons depuis de nombreuses années. Le connecteur RJ45 est remplacé par une antenne. On trouve les clients radio sous la forme de cartes à insérer dans les connecteurs d'une carte mère de PC mais aussi sous forme de clés USB. Ils sont parfois directement intégrés aux ordinateurs portables et sont repérables au petit logo qui ne manque pas d'accompagner cette technologie.

Les points d'accès sont généralement des boîtiers munis de plusieurs antennes (au moins deux) qui sont d'un côté reliés aux clients radio d'une part et à l'infrastructure filaire d'autre part.

L'infrastructure de sécurité est totalement contenue dans le point d'accès ou en partie déportée sur un sous-réseau de l'infrastructure filaire. Elle comprend un ou plusieurs serveurs d'authentification dont le rôle est généralement de contrôler les accès au réseau filaire via les points d'accès sans fil.

Cisco s'est bien entendu intéressé à la technologie sans fil et propose toute une gamme de matériel qui englobe les points d'accès et les clients (gamme *Aironet*) mais aussi divers outils de contrôle et de gestion de l'infrastructure sans fil. Nous allons nous concentrer ici sur les possibilités de configuration (et de sécurisation) d'un point d'accès sans fil tout en donnant pour mémoire des conseils de configuration pour les clients.

© ENI Editions - All rigths reserved - Moha Anisa

Sécurité autour des réseaux sans fil

Comme nous l'avons exposé dans les chapitres précédents, une bonne approche de la sécurité des systèmes d'information consiste à poser quelques exigences (simples) en face desquelles les technologies adéquates sont mises en correspondance.

Exigences de sécurité pour les équipements Wi-Fi	
Exigences	**Techniques**
Sécuriser l'accès au réseau et assurer la confidentialité et l'authenticité des données.	802.1X WPA (*Wireless Protected Access*) EAP (*Extensible Authentication Protocol*) AES mode CCM
Se protéger des attaques par déni de service.	Configuration
Détecter les équipements non autorisés.	WIDS (*Wireless IDS*)
Limiter la portée du signal.	Configuration
Protection physique et logique des équipements radio.	Configuration et installation physique
Interdire les communications entre clients Wi-Fi.	ACL IP et ACL MAC
Séparation des réseaux sans fil et des réseaux d'infrastructure.	Utilisation de VLAN et de Firewall
Limitation du temps et des heures de connexion (avec ou sans trafic).	Configuration

Pour les clients, c'est-à-dire les machines se connectant au réseau sans fil grâce à leur cartes embarquées, nous proposons quelques exigences générales :

Se prémunir contre les connexions entrantes.	Utilisation d'un firewall personnel et d'un anti-virus.
Impossibilité de passer du réseau sans fil au réseau filaire.	Pas d'activation des cartes sans fil et filaire simultanément.
Chiffrement au niveau le plus élevé.	Protocoles de sécurité WPA-2 et AES.
Ne pas accepter de configuration automatique.	Désactiver Windows Zero Configuration.
Ne pas se connecter automatiquement.	Désactivation de la fonctionnalité.

Ces mesures générales sont facilement applicables et aisément compréhensibles d'autant plus que les cas d'attaques sur les ordinateurs portables par le biais du Wi-Fi se sont multipliés dans les lieux publics comme les aéroports. Nous vous conseillons également de vous référer à un exemple de politique de sécurité relative aux stations de travail. Bien que nos exigences le stipulent, nous insistons sur l'interdiction faite aux utilisateurs du réseau d'introduire et de connecter à celui-ci des dispositifs sans fil. Cette bonne pratique n'est hélas parfois pas suivie et certaines architectures filaires se voient dotées de portes de sorties sans fil ruinant potentiellement tout le travail de protection entrepris au préalable.

© ENI Editions - All rigths reserved - Moha Anisa

Sécuriser l'accès au réseau Wi-Fi

Ceci est la première de nos exigences, son objectif est tout comme nous l'avons fait pour les réseaux filaires de conditionner l'accès au réseau (par le biais de la connexion sans fil) à la présentation d'identifiants valides.

Pour illustrer ce propos, nous utiliserons un point d'accès Cisco de type 1230 et un dispositif proche de celui employé pour protéger les accès filaires. En matière de Wi-Fi le maître acronyme à retenir est WPA pour *Wi-Fi Protected Access*. WPA est disponible en deux versions (WPA et WPA-2) et pour chacune d'elles de deux modes (personnel et entreprise).

Initialement, WPA a été conçu afin de remplacer le protocole WEP (*Wired Equivalent Privacy*) dont le modèle de sécurité fut mis à mal peu de temps après sa mise en service. De très nombreux articles existent sur ce sujet ainsi qu'une collection d'outils permettant la récupération des clés de chiffrement seulement après quelques heures d'écoute d'un réseau.

1. WPA

WPA améliora dès sa première mouture le chiffrement utilisé par le protocole WEP en proposant l'utilisation d'une clé plus longue (en fait, il s'agit du vecteur d'initialisation), ainsi qu'un meilleur système de distribution et de dérivation, un meilleur contrôle d'intégrité et l'utilisation d'une clé à chaque paquet chiffré.

WPA- 2 introduit le protocole de chiffrement AES (*Advanced Encryption Standard*) en remplacement de RC4 (utilisé par WEP) avec des clés de 128 bits ainsi qu'une nouvelle collection de systèmes visant à assurer l'intégrité des messages.

WPA entreprise (ou WPA-2 entreprise) : cette version nécessite la mise en place de l'un des protocoles EAP et d'un serveur RADIUS comme nous l'avons décrit dans le cadre de la protection des réseaux filaires. Ici, l'accès est autorisé uniquement après présentation d'un couple utilisateur et mot de passe valide ou d'un certificat personnel de type X509. Le serveur RADIUS prend également en charge la génération et la distribution des clés de chiffrement.

WPA personnel (ou WPA personnel) : dans cette version de WPA, une clé pré-partagée est utilisée entre les participants. Nous pouvons comparer ce mode de fonctionnement à celui d'IPSec qui utilise également une clé partagée. Ce mode est vulnérable en cas de clé mal choisie et ici encore des outils existent pour tenter de deviner la clé notamment en utilisant des dictionnaires contentant des milliers de mots ou de phrases type.

Nous allons utiliser ici pour étudier la protection d'un réseau sans fil le protocole WPA-2 entreprise avec EAP-TLS.

a. WPA-2, EAP-TLS et FreeRADIUS

Nous devrions rajouter AES pour être complet, c'est en effet ce protocole de chiffrement que nous allons employer car c'est le plus puissant mis à disposition. L'utilisation d'EAP-TLS n'est pas chose aisée car elle demande le déploiement et la gestion d'une infrastructure de type PKI. Cela comprend l'émission des certificats et la maintenance de la liste de révocation.

Le principe de fonctionnement choisi dans le cadre de notre étude est :

- de laisser l'utilisateur choisir son réseau Wi-Fi (SSID) ;
- d'authentifier un utilisateur par le biais d'un certificat de type X509 en EAP-TLS en contrôlant que son nom d'utilisateur correspond à celui du certificat ;
- de fournir le VLAN de travail et l'adresse IP dynamiquement en fonction du SSID sur lequel l'utilisateur s'est authentifié.

Nous avons choisi d'utiliser :

- le serveur RADIUS libre FreeRADIUS en remplacement du serveur RADIUS Microsoft que nous avions employé pour l'étude du 802.1X filaire ;
- le client WPA-2 entreprise proposé sous Windows Vista.

Installation du service RADIUS et du certificat client :

L'installation du service RADIUS FreeRADIUS a été accomplie sur une machine Linux Fedora à partir de la simple commande : `# yum install FreeRADIUS`.

Le serveur comporte les fichiers de configuration suivants : *radiusd.conf*, *eap.conf*, *clients.conf*. Ils sont situés dans le répertoire /etc/raddb/.

© ENI Editions - All rigths reserved - Moha Anisa

```
  eap {

    default_eap_type = tls
    timer_expire     = 60
    ignore_unknown_eap_types = no
    cisco_accounting_username_bug = yes
    tls {
      certdir = ${confdir}/certs
      cadir = ${confdir}/certs
      private_key_password = whatever
      private_key_file = ${certdir}/server.pem
      certificate_file = ${certdir}/server.pem
      CA_file = ${cadir}/ca.pem
      dh_file = ${certdir}/dh
      random_file = ${certdir}/random
      fragment_size = 1024
      check_crl = yes
      CA_path=${certdir}/WIFIcrl.pem
      check_cert_issuer="/C=FR/L=Toulouse/O=TESTLAB"
      check_cert_cn = %{User-Name}
      cipher_list = AES256-SHA
    }

      }
```

Le fichier *radiusd.conf* n'a pas été modifié et nous donnons ici la configuration du fichier *eap.conf* qui comme son nom l'indique configure les protocoles EAP.

Nous observons :

- Les noms et les emplacements des divers certificats nécessaires c'est-à-dire celui de l'autorité de certification (CA) et du serveur RADIUS dont la phrase de sécurité figure en clair dans la configuration.

- La liste de révocation (CRL) est ici configurée afin de rejeter tout certificat qui s'y trouverait. Il est à ce propos indispensable de configurer la CA pour que son certificat puisse signer une CRL. Nous vous invitons à vous rapprocher de la configuration de votre PKI. Dans le cas d'*OpenSSL* la commande `keyUsage = cRLSign` est nécessaire dans le fichier de configuration.

- Enfin, nous testons quelques attributs du certificat, le nom d'utilisateur présenté et nous forçons le protocole de chiffrement AES.

Une seule modification intéresse le fichier *clients.conf* et consiste à déclarer le point d'accès sans fil comme client RADIUS avec son adresse réseau et son secret.

```
Client 192.168.1.16 {
  secret = cisco
}
```

Il est ensuite indispensable de configurer des certificats sur lesquels s'appuie le protocole EAP-TLS. Ces fichiers sont dans le répertoire */etc/raddb/certs* et doivent posséder des droits permettant au serveur FreeRADIUS de les lire.

Sont nécessaires :

- Un certificat auto signé pour simuler une autorité de certification (CA) au format *der* et de l'installer dans le magasin nommé autorités principales de confiance. Pour mémoire les certificats sont importés à partir d'Internet Explorer en suivant le chemin : **Outils - Options Internet - Contenu - Certificats - Importer**.

- Un certificat pour le serveur RADIUS signé par cette autorité de certification. Un script fourni avec *FreeRADIUS* dans le répertoire */certs* permet de créer les certificats de l'autorité de certification et du serveur (ces deux premiers certificats sont créés avec les commandes : `make ca` et `make server`).

- un certificat pour le client également signé par cette même autorité de certification. Ce certificat est émis sous la forme d'un fichier dont l'extension est de type .p12 avant d'être chargé dans le magasin nommé Personnel. Il est créé avec les commandes suivantes :

```
openssl req -new -out client.csr -keyout client.key -
```

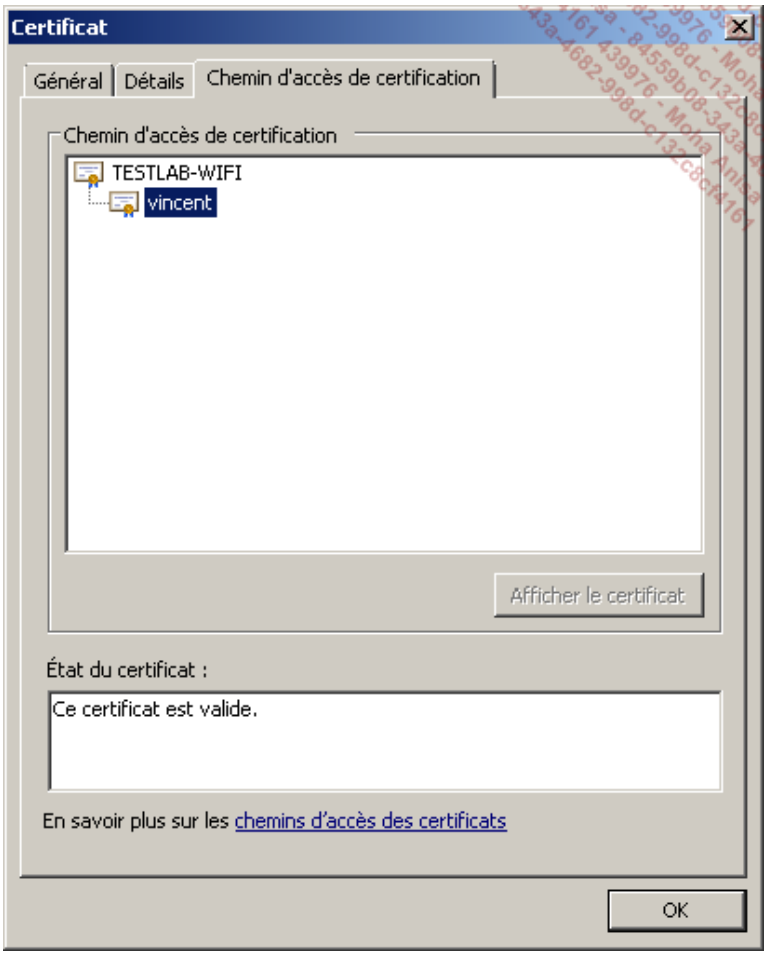

© ENI Editions - All rigths reserved - Moha Anisa

```
config ./client.cnf

openssl x509 -req -in client.csr -out client.crt -CA
ca.pem
-CAkey ca.key -CAserial serial

openssl pkcs12 -export -inkey client.key -in client.crt -
out client.p12
```

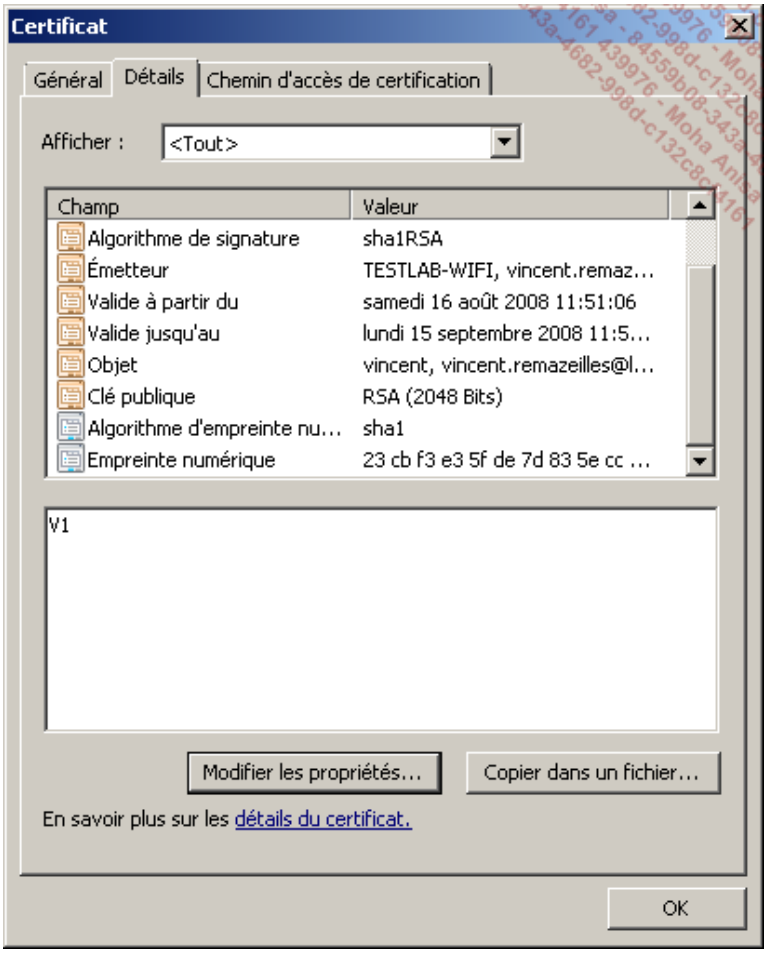
Il est important de mentionner que dans notre cas, le certificat client est directement signé par l'autorité de certification sans passer par une autorité intermédiaire ce qui est généralement le cas. Cela implique de ne pas partager cette autorité de certification avec une autre organisation qui (si tel était le cas) pourrait signer des certificats valides à votre place. Dans cet exemple, cela ne pose aucun problème.

Si en plus de la CA racine, il existe une CA intermédiaire, les deux certificats devront être rassemblés dans un seul fichier qui sera déclaré avec la commande `CA_file =` du fichier eap.conf. Un certificat n'est que rarement délivré par une CA racine. Il l'est généralement par l'intermédiaire d'une CA intermédiaire. Si tel est le cas, le certificat de la CA racine et de la CA intermédiaire doivent être fusionnés dans un fichier unique. Ce fichier sera déclaré dans le fichier eap.conf avec la commande "`CA_file=`". Pour mémoire, la commande UNIX qui permet de concaténer deux fichiers est : cat fichier_1 fichier_2>fichier_3.

Soulignons de même qu'il est fortement recommandé lors de l'importation du certificat client de cocher l'option afin que la phrase de protection de la clé privée soit demandée systématiquement lors de l'utilisation du certificat.



© ENI Editions - All rigths reserved - Moha Anisa



Nous observons sur ces deux images d'un même certificat client la chaîne de certification et le détail des champs. Comme indiqué, ce certificat a été directement signé pour l'utilisateur « Vincent » par l'autorité de certification TESTLAB-WIFI.

Configuration du point d'accès sans fil (AP 1231G) :

```
hostname ap
!
aaa new-model
aaa group server radius rad_eap
 server 192.168.1.3 auth-port 1812 acct-port 1813
aaa authentication login eap_methods group rad_eap
aaa session-id common
!
dot11 ssid EAP-TLS
    authentication open eap eap_methods
    authentication network-eap eap_methods
    authentication key-management wpa
!
username vincent privilege 15 secret5 $3HBC$EpW82SUbZNtmI3PG0rU2z
!
bridge irb
!
interface Dot11Radio0
  no ip address
  no ip route-cache
  encryption mode ciphers aes-ccm
  broadcast-key change 1800
  ssid EAP-TLS
  bridge-group 1
!
interface FastEthernet0
  bridge-group 1
!
interface BVI1
```


© ENI Editions - All rigths reserved - Moha Anisa

```
  ip address 192.168.1.16 255.255.255.0
!
ip radius source-interface BVI1

!
radius-server host 192.168.1.3 auth-port 1812 acct-port 1813 key 7
13061E010803
bridge 1 route ip
```

Bien que les points d'accès Cisco bénéficient d'une interface graphique, nous présentons ici la configuration en mode texte pour des raisons pratiques.

Les cinq premières lignes configurent le système AAA (*Authentication Authorization Accounting*) sur le point d'accès dont nous voyons au passage qu'il se configure comme un routeur. Pour mémoire la commande `aaa new-model` active les fonctions d'authentification externalisées sous la responsabilité de serveurs de type RADIUS ou TACACS. Le serveur radius est une première fois défini au sein d'un groupe (`rad_eap`) avec le nom de la méthode pour s'y référer (`eap_methods`).

Le SSID (`EAP-TLS`) est l'identifiant du réseau sans fil. C'est le nom du réseau qui s'affiche lorsque ce dernier est découvert par le système d'exploitation au voisinage du point d'accès. Le SSID appelle la méthode `eap_methods` laquelle, nous venons de le voir, se réfère au groupe `radius rad_eap`. WPA est choisi à ce niveau.

Détaillons à présent un groupe de commande particulier.

La commande `bridge irb` permet de configurer le point d'accès (qui est à la base un routeur) de telle sorte qu'il se comporte comme un pont (en anglais bridge). Le point d'accès devient donc l'équivalent d'un commutateur Ethernet muni de deux interfaces physiques (radio et filaire) entre lesquelles les paquets vont transiter. Il est nécessaire de déclarer les interfaces qui participent à ce processus en incluant dans leur configuration la commande : `bridge-group 1`. Nous trouvons bien celle-ci sur l'interface radio et sur l'interface Ethernet.

L'interface *BVI* (*Bridge-group Virtual Interface*) possède une interface routée par laquelle le point d'accès est joignable pour les tâches administratives. Cette interface représente le pont tout comme l'interface d'administration d'un commutateur Ethernet. Le numéro de l'interface *BVI* (1 dans notre cas) est le lien avec le numéro du *bridge-group* (1 également).

La commande `bridge 1 route ip` indique qu'une interface IP est présente et que le trafic IP entrant lui est destiné.

L'interface *dot11radio0* est configurée pour mettre en œuvre le chiffrement des informations avec le protocole AES (aes-ccm) puis est rattachée au SSID EAP-TLS. Elle participe au pont avec la commande décrite précédemment.

L'interface Ethernet participe au pont grâce à la même commande.

Viennent au final les commandes permettant la communication avec le serveur RADIUS. Deux commandes sont présentes. La commande `ip radius source-interface BVI1` permet au point d'accès de communiquer avec le serveur RADIUS par le biais de l'adresse IP affectée à l'interface BVI. La commande `radius-server host` donne l'adresse IP du serveur RADIUS ainsi que le secret partagé. Attention aux valeurs des ports qui par défaut sur le point d'accès ne correspondent par toujours aux valeurs par défaut du serveur FreeRADIUS.

Notons qu'aucune commande visant à configurer l'adresse IP du client final (DHCP) n'est ici présente. Ceci est du au rôle de pont (bridge) tenu par le point d'accès.

Fonctionnement du serveur RADIUS :

```
/usr/sbin/radiusd -X

FreeRADIUS Version 2.0.5, for host i386-redhat-linux-gnu, built on
Jul 30 2008 at 10:41:14
Copyright (C) 1999-2008 The FreeRADIUS server project and
contributors.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License v2.
Starting - reading configuration files ...

Listening on authentication address 192.168.1.3 port 1812
```

La commande figurant en premier dans la capture ci-dessus, permet de lancer le serveur RADIUS à la main en activant la visualisation des évènements. Si la configuration s'avère correcte, le serveur se met en écoute sur le port 1812. La capture a été volontairement tronquée.

```
rad_recv: Access-Request packet from host 192.168.1.16 port 1645,
id=22, length=127
  User-Name = "vincent"
```

© ENI Editions - All rigths reserved - Moha Anisa

```
  Framed-MTU = 1400
  Called-Station-Id = "001b.53ba.46d0"
  Calling-Station-Id = "001f.3c05.653c"
  Service-Type = Login-User
  Message-Authenticator = 0xd2135a7903682b3398591113c2565c66
  EAP-Message = 0x0202000c0176696e63656e74
  NAS-Port-Type = Wireless-802.11
  NAS-Port = 265
  NAS-IP-Address = 192.168.1.16
  NAS-Identifier = "ap"
```

Nous observons ici l'arrivée d'une requête en provenance de notre point d'accès. Y figurent le nom de l'utilisateur ainsi que l'adresse IP et le nom (ap) du point d'accès.

```
auth: type "EAP"
+- entering group authenticate
  rlm_eap: Request found, released from the list
  rlm_eap: EAP/tls
  rlm_eap: processing type tls
  rlm_eap_tls: Authenticate
  rlm_eap_tls: processing TLS
  TLS Length 108
rlm_eap_tls:  Length Included
  eaptls_verify returned 11
    (other): before/accept initialization
    TLS_accept: before/accept initialization
  rlm_eap_tls: <<< TLS 1.0 Handshake [length 0067], ClientHello
    TLS_accept: SSLv3 read client hello A
  rlm_eap_tls: >>> TLS 1.0 Handshake [length 004a], ServerHello
    TLS_accept: SSLv3 write server hello A
  rlm_eap_tls: >>> TLS 1.0 Handshake [length 085a], Certificate
    TLS_accept: SSLv3 write certificate A
  rlm_eap_tls: >>> TLS 1.0 Handshake [length 00a5],
CertificateRequest
    TLS_accept: SSLv3 write certificate request A
    TLS_accept: SSLv3 flush data
    TLS_accept: Need to read more data: SSLv3 read client
certificate A
In SSL Handshake Phase
```

Le client et le serveur RADIUS par l'intermédiaire du point d'accès mettent en œuvre le protocole EAP-TLS. Le certificat serveur est présenté et le serveur RADIUS demande au client Wi-Fi de présenter le sien.

```
--> User-Name = vincent
--> BUF-Name = vincent
--> subject = /C=FR/ST=Midi-
Pyrenees/L=Toulouse/O=TESTLAB/emailAddress=vincent.remazeilles
@laposte.net/CN=vincent
--> issuer  = /C=FR/ST=Midi-
Pyrenees/L=Toulouse/O=TESTLAB/emailAddress=vincent.remazeilles
@laposte.net/CN=TESTLAB-WIFI
--> verify return:1
    TLS_accept: SSLv3 read client certificate A
  rlm_eap_tls: <<< TLS 1.0 Handshake [length 0106],
ClientKeyExchange
    TLS_accept: SSLv3 read client key exchange A
  rlm_eap_tls: <<< TLS 1.0 Handshake [length 0106],
CertificateVerify
    TLS_accept: SSLv3 read certificate verify A
  rlm_eap_tls: <<< TLS 1.0 ChangeCipherSpec [length 0001]
  rlm_eap_tls: <<< TLS 1.0 Handshake [length 0010], Finished
    TLS_accept: SSLv3 read finished A
  rlm_eap_tls: >>> TLS 1.0 ChangeCipherSpec [length 0001]
    TLS_accept: SSLv3 write change cipher spec A
  rlm_eap_tls: >>> TLS 1.0 Handshake [length 0010], Finished
    TLS_accept: SSLv3 write finished A
    TLS_accept: SSLv3 flush data
    (other): SSL negotiation finished successfully
SSL Connection Established
  eaptls_process returned 13
```


© ENI Editions - All rigths reserved - Moha Anisa

```
...
...

  rlm_eap_tls: processing TLS
rlm_eap_tls: Received EAP-TLS ACK message
  rlm_eap_tls: ack handshake is finished
  eaptls_verify returned 3
  eaptls_process returned 3
  rlm_eap: Freeing handler
++[eap] returns ok
```

Le certificat client est ici examiné et accepté mettant fin avec succès à l'échange SSLv3 entre le client Wi-Fi et le serveur RADIUS.

Nous venons de décrire une configuration basée sur EAP-TLS entre un client Wi-Fi et un serveur RADIUS par l'intermédiaire d'un point d'accès de type 1231. EAP-TLS n'est pas le seul protocole disponible pour ce genre d'authentification. Le protocole PEAP que nous avions décrit précédemment est parfaitement efficace et plus simple à déployer car il ne nécessite pas de certificats clients. PEAP et EAP-TLS sont disponibles avec les versions courantes du système d'exploitation Windows.

2. LWAPP

Les réseaux sans fil sont victimes d'attaques visant principalement à déconnecter les clients en cours de session ou à perturber le lien radio par l'envoi d'ondes électromagnétiques puissantes, concentrées et dirigées vers les points d'accès sans fils. D'autres attaques sont dirigées vers les stations de travail dans le but de détourner l'utilisateur d'un point d'accès officiel pour le rediriger vers un point d'accès maquillé par l'attaquant. Ces attaques se déroulent en deux temps. L'utilisateur est tout d'abord forcé à se déconnecter du point d'accès légitime puis invité à se connecter à un point d'accès contrôlé par l'attaquant. Enfin, existent des attaques directes pour lesquelles l'ordinateur cible est directement victime de l'attaque.

Les points d'accès sans fil de Cisco sont des ponts Ethernet qui ne possèdent pas nativement l'intelligence nécessaire à la détection des attaques que nous venons de citer. Les points d'accès sont considérés comme des équipements isolés dont l'administration n'est pas centralisée. Il en est de même pour le rassemblement des journaux d'évènements. En l'état, la détection des attaques est rendue très difficile.

Afin de compléter sa gamme avec une solution de sécurité cohérente et intégrée au maximum, Cisco propose des équipements complémentaires et un protocole de communication spécifique.

Le protocole LWAPP est la première brique de cette approche de la gestion des points d'accès Wi-Fi. Il permet de centraliser les tâches de configuration, de surveillance et de dépannage. Les tâches de configuration comprennent la mise en place et le déploiement de politique de sécurité sous forme d'ACL. Un autre point que nous allons aborder est la gestion des ondes radios. Avec le protocole LWAPP, l'administrateur d'un réseau Wi-Fi a la possibilité de gérer (d'une manière centralisée) les puissances d'émission des points d'accès. En matière de détection des intrusions, le protocole LWAPP se charge de centraliser les informations en provenance des fonctionnalités de sondes IDS disponibles sur les points d'accès.

Deux équipements se démarquent dans la gamme des produits de gestion des réseaux sans fil. Ce sont le contrôleur de réseau WLC (*Wireless Lan Controler*) et le WCS (*Wireless Control System*). Le WLC est un commutateur Ethernet basé entre autre sur le châssis du Catalyst 3750. Il est possible d'empiler les WLC pour augmenter la capacité de traitement des points d'accès sans fil. Le WLC doit être abordé comme le dépositaire des politiques Wi-Fi de l'organisation en matière de sécurité, de gestion des signaux radio, de qualité de service et de gestion de la mobilité. La mobilité est la capacité pour un utilisateur de se déplacer munis d'un équipement terminal Wi-Fi sans devoir se réauthentifier lors de ses déplacements entre plusieurs zones de couvertures.

Le WCS est une suite logicielle comprenant une base de données et des applications web qui offrent la possibilité de planifier avec précision les zones de couverture d'une zone par des points d'accès. Le réseau une fois opérationnel est alors étroitement surveillé. L'application web, sous forme d'un portail, présente des informations statistiques et des vues en temps réel de la couverture radio et de tous les incidents. Un service de géolocalisation est également disponible afin de connaître si le besoin s'en fait sentir la position de n'importe quel client sans fil. Pour conclure sur ce logiciel, la sécurité est prise en compte avec des signatures d'attaques (créations de signatures) et la détection de points d'accès non autorisés (*rogue access points*). Pour de plus amples informations, nous vous invitons à consulter le site Internet de Cisco.

© ENI Editions - All rigths reserved - Moha Anisa

Ces équipements aux capacités et aux fonctionnalités remarquables sont relativement coûteux et l'investissement qu'ils représentent doit être compensé par les services qu'ils offrent. L'image montre une page du logiciel WCS sur laquelle sont disponibles divers rapports concertant la sécurité.

La géolocalisation et la gestion centralisée de la couverture radio sont l'apanage de solutions réservées aux réseaux comprenant plusieurs dizaines voire centaines de points d'accès. Toutefois, il est parfaitement envisageable avec des moyens limités au seul point d'accès de pratiquer l'étude de la couverture radio d'un bâtiment.

3. Protection autonome

Une de nos exigences de sécurité est de limiter la portée du signal afin que le réseau radio soit le plus possible hors de portée de personnes mal intentionnées. Il est tout à fait envisageable de déterminer son périmètre de travail (et de sécurité) avec une machine de votre parc équipée d'une carte réseau Wi-Fi à vos standards.

En se déplaçant méthodiquement avec cette machine tout en ayant non moins méthodiquement placé un point d'accès sans fil, vous tracerez sur un plan les valeurs du signal capté par votre carte réseau tout au long de votre parcours. Le but de l'exercice est de fournir un signal radio aux utilisateurs en évitant le chevauchement des fréquences tout en ne débordant pas du périmètre fixé.

Toujours en fonction de la politique de sécurité il est toléré ou non que les signaux dépassent du périmètre des bâtiments. Ici encore les réglages des puissances d'émission sont ajustés en fonction des besoins. L'objectif fixé par la politique de sécurité peut tout à fait imposer qu'aucun signal ne puisse être capté dans le domaine public avec un matériel conventionnel. Hélas, des techniques existent pour améliorer considérablement la précision et la directivité des antennes Wi-Fi afin de recevoir des signaux lointains et affaiblis durant leur transmission. Nous entrons ici dans le domaine des écoutes illicites.

La puissance d'émission des points d'accès sans fils est modifiable dans la configuration et il est également possible au point d'accès d'imposer une puissance d'émission au client sans fil en passe de se connecter.

```
ap(config)#int dot11Radio 0
ap(config-if)# power local ?
  cck   Set local power for CCK rates
  ofdm  Set local power for OFDM rates

ap(config-if)# power local cck ?
  <1 - 50>  One of: 1 5 10 20 30 50
  maximum   Set local power to allowed maximum

ap(config-if)# power local ofdm ?
  <1 - 30>  One of: 1 5 10 20 30
  maximum   Set local power to allowed maximum
```


© ENI Editions - All rigths reserved - Moha Anisa

Chaque type de modulation (CCK et OFDM) possède une gamme de réglage pour la puissance d'émission. Les valeurs sont données en mW (milliwatt). Le mot clé pour configurer la puissance d'émission du point d'accès est local.

```
ap(config)#int dot11Radio 0
ap(config-if)#power client ?
  <1 - 50>  One of: 1 5 10 20 30 50
  local     Set client power to Access Point local power
  maximum   Set client power to allowed maximum
```

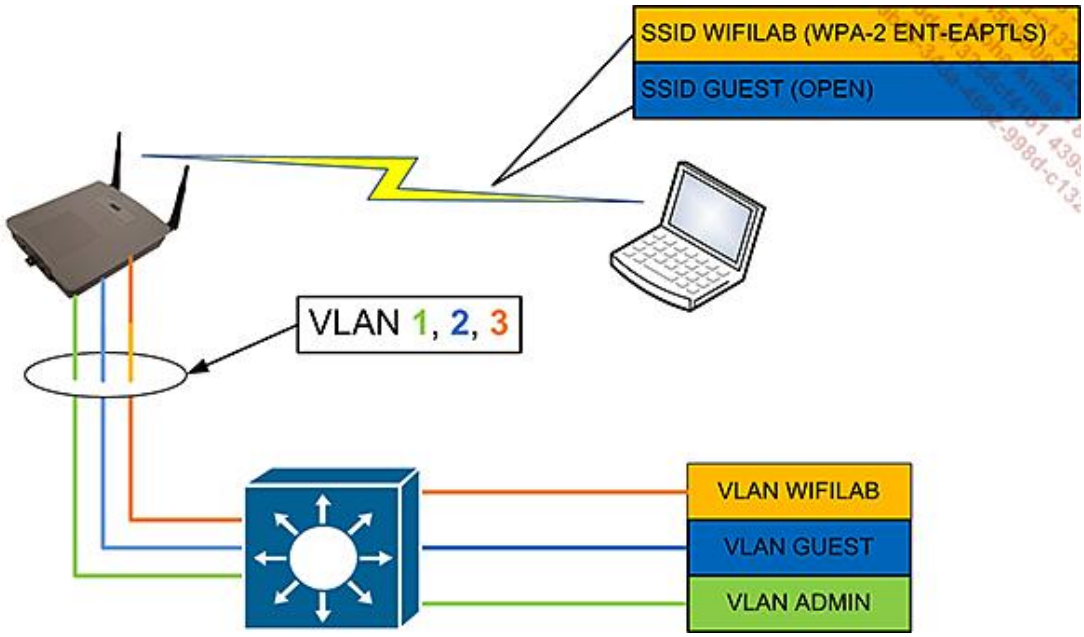
Ici nous observons les possibilités de réglage de la puissance d'émission du client imposées par le point d'accès.

Avec ce petit panel de commandes, il est à présent envisageable de régler finement les puissances d'émission afin de rester dans le périmètre imposé par la politique de sécurité.

4. Limitations de connexion

Nous savons qu'un point d'accès sans fil est un pont accomplissant sa tâche au niveau 2 du modèle OSI. Ceci implique si rien n'est entrepris une connectivité totale entre les clients sans fil ayant réussi à se rattacher au point d'accès. Ceci est tout à fait concevable si l'on désire mettre en service un réseau entièrement ouvert au sein duquel tout un chacun a la possibilité de communiquer avec tous les membres connectés. Mais, dans le monde de l'entreprise et du service, cette approche n'est pas de mise et les politiques de sécurité imposent (la plupart du temps) une limitation stricte des communications.

Notre point d'accès sans fil va recevoir une configuration limitant son enclin naturel qui consiste à relier entre eux tous les clients sans fil et de les connecter ensemble au reste du réseau filaire.



Les points d'accès Cisco offrent la possibilité d'associer les *VLAN* au SSID. Un résumé extrêmement bref serait d'énoncer le principe suivant : « À chaque SSID son *VLAN*, sa méthode d'authentification propre et sa plage d'adresses IP » Ceci est très séduisant. Le schéma ci-dessus nous montre une telle configuration.

Ici nous observons :

- un transporteur de VLAN sur un lien physique unique aussi appelé trunk qui relie un point d'accès à un commutateur doté de fonctions de routage ;
- deux SSID proposés par le point d'accès et correspondant aux VLAN Wi-FiLAB et GUEST ;
- pour chaque SSID qu'une politique d'authentification spécifique est proposée ;
- sur l'équipement d'infrastructure : les deux *VLAN* précités et le VLAN d'administration (hébergeant le serveur RADIUS par exemple).

Les étendues DHCP mises à la disposition des clients ne sont pas représentées pour des raisons de clarté sur le schéma. Examinons la configuration du point d'accès.

© ENI Editions - All rigths reserved - Moha Anisa

```
ap(config-if)#int dot11Radio 0.1
ap(config-subif)#encapsulation ?
  dot1Q  IEEE 802.1Q Virtual LAN

ap(config-subif)#encapsulation dot1
ap(config-subif)#encapsulation dot1Q ?
  <1-4094>  IEEE 802.1Q VLAN ID

ap(config-subif)#encapsulation dot1Q 1 ?
  native        Make this as native vlan
  second-dot1q  Configure this subinterface as a 1Q-in-1Q
subinterface
  <cr>
ap(config-subif)#encapsulation dot1Q 1 native
ap(config-subif)#exit

------------------------------------------------------------

ap(config-if)#int f0.1
ap(config-subif)#enca
ap(config-subif)#encapsulation dot
ap(config-subif)#encapsulation dot1Q 1 native
```

Tout d'abord nous configurons une sous-interface sur l'interface radio. Pour mémoire une sous interface est créée lorsque l'on fait directement suivre la désignation de l'interface par un point suivi d'un chiffre qui désigne le numéro d'ordre de la sous-interface. Ici, nous créons la sous-interface numéro 1 et nous l'affectons au *VLAN* 1 en indiquant de surcroit qu'il s'agit du VLAN natif.

Puis, à l'identique une sous-interface est créée sur l'interface filaire. Elle est également rattachée au *VLAN* 1. Ces deux sous-interfaces membres du *VLAN* 1 sont automatiquement liées au `bridge-group 1` précédemment créé. Rappelons que ce même `bridge-group 1` est lié à l'interface BVI1.

Tout ceci peut sembler confus, mais il faut garder à l'esprit que Cisco utilise fréquemment dans les configurations les chiffres et les mots-clés pour lier les commandes entre elles.

```
!
interface FastEthernet0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 no bridge-group 2 source-learning
 bridge-group 2 spanning-disabled
!
interface FastEthernet0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 no bridge-group 3 source-learning
 bridge-group 3 spanning-disabled
```

Voici un extrait de la configuration des sous-interfaces filaires numéro 2 et 3 rattachées aux VLAN 2 et 3.

```
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
 bridge-group 2 spanning-disabled
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 block-unknown-source
```


© ENI Editions - All rigths reserved - Moha Anisa

```
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
 bridge-group 3 spanning-disabled
```

Ici, nous observons dans cet extrait la configuration correspondante sur les sous-interfaces radio.

```
ap(config)# dot11 ssid WIFILAB
ap(config-ssid)# vlan 2
ap(config-ssid)# authentication open eap eap_methods
ap(config-ssid)# authentication network-eap eap_methods
ap(config-ssid)# authentication key-management wpa

---------------------------------------

ap(config)# dot11 ssid GUEST
ap(config-ssid   vlan 3
ap(config-ssid   authentication open
ap(config-ssid   mbssid guest-mode
```

Ici, les deux SSID sont créés et associés respectivement aux VLAN 2 et 3. Sont aussi précisés les modes et méthodes d'authentification.

```
ap(config)#interface Dot11Radio 0
ap(config-if)# encryption mode ciphers aes-ccm
ap(config-if)# encryption vlan 2 mode ciphers aes-ccm
ap(config-if)# broadcast-key change 1800 membership-termination
capability-change
ap(config-if)# broadcast-key vlan 2 change 1800 membership-
termination capability-change
ap(config-if)# ssid GUEST
ap(config-if)# ssid WIFILAB
```

Les deux SSID précédemment créés sont associés à l'interface radio principale. Le mode de chiffrement que nous avions préalablement choisi est conservé.

En face de cette configuration, il faut :

- disposer un équipement de niveau 3 recevant le trunk sur une interface physique ;
- créer des interfaces de type VLAN qui font office de passerelle par défaut pour les clients des SSID ;
- associer à chaque interface *VLAN* un service DHCP pour les clients sans fil.

```
interface FastEthernet0/1
  switchport trunk allowed vlan 1-3
  switchport mode trunk
  spanning-tree portfast
```

L'interface est présentement configurée pour accueillir les VLAN de 1 à 3.

```
vlan 2
  name WIFILAB
!
vlan 3
  name GUEST
!
interface Vlan1
  ip address 192.168.1.254 255.255.255.0
  no ip route-cache
!
interface Vlan2
  ip address 192.168.2.254 255.255.255.0
  no ip route-cache
  !
interface Vlan3
  ip address 192.168.3.254 255.255.255.0
  no ip route-cache
```

© ENI Editions - All rigths reserved - Moha Anisa

Les deux *VLAN* WIFILAB et GUEST sont activés avec les trois interfaces VLAN. Les adresses IP sont les passerelles par défaut des clients sans fil raccordés à ces *VLAN*. Le *VLAN* 1 dans notre cas n'est pas créé car il existe toujours.

```
service dhcp
!
ip dhcp excluded-address 192.168.2.254
ip dhcp excluded-address 192.168.3.254
!
ip dhcp pool WIFILAB
   network 192.168.2.0 255.255.255.0
   dns-server 192.168.4.1
   default-router 192.168.2.254
!
ip dhcp pool GUEST
   network 192.168.3.0 255.255.255.0
   default-router 192.168.3.254
   dns-server 192.168.4.1
```

Le service DHCP est activé sur l'équipement de niveau 3 (`service dhcp`) puis les adresses des passerelles par défaut sont exclues des étendues afin de ne pas se voir affectées à un client.

Deux étendues (`dhcp pool`) sont activées et référencent pour chacun des *VLAN* la passerelle par défaut ainsi qu'un serveur DNS commun. Le lien entre les étendues DHCP et les interfaces de type *VLAN* s'effectue sur la correspondance entre les adresses de réseau des étendues (`network`) et les adresses IP des interfaces Vlan.

Un problème se pose toutefois à ce niveau. Si rien n'est fait, les membres du *VLAN* WIFILAB et GUEST peuvent échanger des paquets ce qui n'est pas souhaitable. Ce phénomène est naturel car l'équipement de niveau trois route nativement entre ses interfaces. Les ACL une fois encore viennent dénouer la situation. Cependant, les clients au sein d'un *VLAN* sur le point d'accès ont encore la possibilité de dialoguer entre eux ce qui n'est pas conforme aux exigences de sécurité. De nouvelles *ACL* seront positionnées sur les interfaces routées. Enfin, les clients sans fils ne sauraient communiquer avec une autre adresse source que celle qui leur a été communiquée. Faisons le point en nous posant comme observateur des paquets en transit sur l'interface *VLAN*. Il ne reste plus qu'à traduire le tableau suivant en *ACL* de type étendues.

Adresse IP Source du client sans fil fournie par DHCP.	Autorisé
Adresse IP Source du client sans fil non conforme.	Interdit
Adresse IP de destination correspondant à une adresse locale au VLAN d'appartenance.	Interdit
Adresse IP de destination non locale au VLAN et autorisée par la politique de sécurité.	Autorisé

5. Timeouts

La dernière exigence stipule (à demi-mots) qu'un client inactif durant un certain temps doit être déconnecté du réseau. Dans le même esprit on désire limiter l'accès au réseau sans fil à certaines plages horaires.

La commande `dot1x reauth-period` en mode général permet de forcer un client authentifié à se réauthentifier en fonction du temps paramétré.

Pour limiter l'accès au réseau sans fil, une méthode consiste à positionner une ACL associée à une condition de temps (*time based ACL*). Ceci est intéressant pour limiter l'accès des invités (voire des employés) au-delà d'une certaine heure.

6. Autres mesures

Le champ des mesures de protection des réseaux sans fil est si vaste que Cisco a intégré dans sa gamme de produits une solution de sonde IDS (*Intrusion Detection System*) basée sur l'analyse comportementale du trafic passant par les points d'accès ou capté par eux. Les tentatives de reconnaissance du réseau sont ainsi détectées et signalées sous forme d'une alarme. Pour ce faire les points d'accès sans fil peuvent être configurés afin d'officier comme des sondes passives à l'écoute du réseau radio dans leur périmètre.

La solution porte le nom de WCS (*Wireless Control System*), elle se compose d'un service à installer sous Microsoft Windows ou *Linux Redhat Enterprise 5* et d'une interface d'administration.

Le point d'accès sans fil que nous avons utilisé peut être configuré afin de participer à un réseau de sonde IDS sans fil, après avoir déclaré son rattachement à une station WDS le point d'accès est configuré en mode *scanner* ou en

© ENI Editions - All rigths reserved - Moha Anisa

mode *monitor*. Le mode scanner surveille tous les canaux alors qu'en mode monitor, le point d'accès ne surveille que le canal sur lequel il est configuré.

© ENI Editions - All rigths reserved - Moha Anisa

Conclusion

Les connexions sans fil aux réseaux d'entreprise ou à Internet sont très populaires et disponibles sur une gamme étendue de matériels à commencer par les ordinateurs personnels, mais aussi les assistants personnels et certains modèles de téléphones. Le modèle de sécurité du Wi-Fi a connu dès ses débuts de graves problèmes de sécurité dont il hérite encore à cause de la compatibilité descendante que le protocole se doit de maintenir. WEP est toujours disponible alors que son utilisation n'est franchement pas recommandée.

Fort heureusement, la situation s'est considérablement améliorée avec la mise en service des protocoles WPA notamment dans leur version entreprise. La condition sine qua non à une amélioration de la sécurité des réseaux sans fil est de déployer systématiquement ces principes en les couplant à des mécanismes d'authentification forte. Ici, les serveurs RADIUS adossés à des bases de comptes comme Active Directory ou de jetons à usage unique sont recommandés.

Un point primordial est aussi la prise de conscience collective et individuelle des risques liés à l'installation non autorisée de points d'accès ou de cartes réseau sans fil. Ces initiatives malheureuses entravent et vont à l'encontre de toutes les mesures de protection que nous venons d'évoquer.

© ENI Editions - All rigths reserved - Moha Anisa

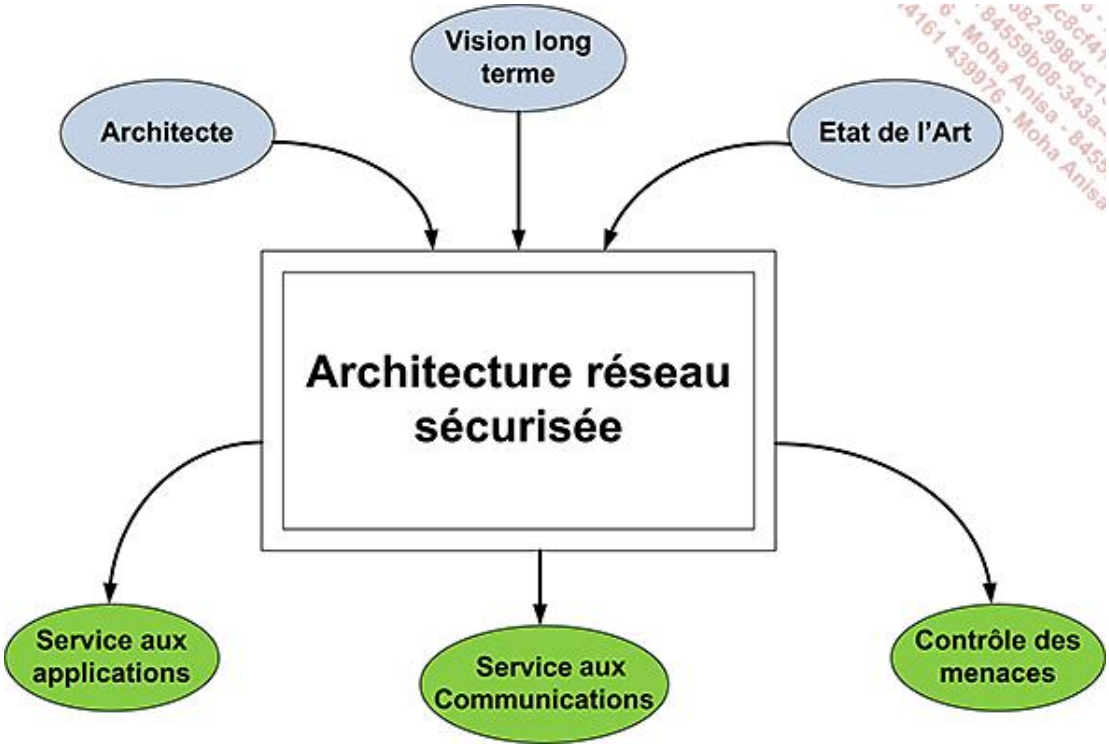
L’architecture réseau et sécurité

Un réseau est soumis régulièrement à de nombreuses évolutions et modifications qui sont le fruit d’une réflexion impliquant le travail du service d’architecture. Les entreprises les plus modestes ne sont pas dotées d’un tel service qui reste en règle générale l’apanage des groupes plus grands. Toutefois, la réflexion sur les tenants et les aboutissants d’une évolution relève de la même logique. Ce travail soulève principalement des questions concernant l’impact des modifications sur l’existant et la manière de procéder à l’intégration. Les tâches du service d’architecture s’il existe sont réparties autour de pôles liés aux spécialités qui composent le système d’information et nous y trouvons tout naturellement des spécialistes de la sécurité et des réseaux. Pour ces personnes, une connaissance approfondie de l’existant est impérative préalablement à toute étude d’évolution du réseau. Pour les entreprises de taille modeste, le responsable informatique fait office d’architecte et prend conseil auprès de ressources extérieures tout en restant maître de ses choix.

Les réseaux ont bénéficié ces dernières années d’avancées technologiques dans le domaine de la sécurité. Citons au passage les protections diverses et variées face à l’Internet, l’avènement de la téléphonie sur IP et des réseaux sans fil. De nos jours, de nombreuses sociétés ouvrent leur réseau à leurs partenaires dans le but de leur permettre d’accéder à des applications ou à des documents. Tout ceci soulève de multiples questions auxquelles les architectes du domaine réseau et sécurité sont sommés de répondre pour ne pas compromettre la bonne marche de l’entreprise.

Une approche méthodique consiste à scinder l’architecture globale en zones fonctionnelles recevant chacune un niveau de sécurité en fonction de sa position et de son rôle.

Les techniques que nous avons abordées lors des chapitres précédents vont ici être mise à contribution. À chaque zone de sécurité nous ferons correspondre un jeu de mesures techniques et organisationnelles.



Il est important de comprendre qu’au-delà de la protection du seul réseau, l’architecture de sécurité a pour objectif ultime la disponibilité des applications et des données. Le schéma montre en entrée (bulles supérieures) les composantes de l’architecture sécurisée et en sortie de celle-ci, les services fournis aux divers processus déployés par l’entreprise.

Nous allons présenter dans ce chapitre les zones de sécurité qui connectées les unes aux autres constituent le réseau sécurisé dans son entièreté. Nous allons mettre en correspondance pour chacune des zones les fonctions de sécurité abordées au cours des chapitres précédents.

© ENI Editions - All rigths reserved - Moha Anisa

La vision de Cisco

Cisco présente un concept nommé "*the self-defending Network*", le réseau qui se défend seul, le réseau à auto défense. Cette approche de la sécurité des réseaux s'étend à toutes les couches du modèle OSI et offre des services sécuritaires aux équipements, aux utilisateurs et aux applications. Cette offre est étroitement connectée à des systèmes de contrôle et de surveillance. Ce concept se décline en solutions c'est-à-dire en produits qui sont intégrés à l'architecture réseau. Il en résulte une architecture réseau sécurisée.

Les trois grandes familles de solutions introduites par Cisco sont :

- le contrôle des menaces pour les infrastructures, les équipements d'extrémité et la messagerie dont les produits entre autres englobent : les pare-feu, les systèmes de prévention et de détection d'intrusion, les contrôleurs d'accès au réseau, les agents de sécurité, les passerelles de messagerie ;
- la sécurité des communications dont les produits fournissent des services IPSec ou VPN SSL : ce sont les routeurs et les pare-feu ;
- le contrôle d'accès au réseau avec l'équipement NAC (*Network Access Control*) qui contrôle la sécurité des équipements voulant se connecter au réseau.

Ces trois grandes familles de produits sont réparties sur des zones de sécurité qui correspondent aux zones de ségrégation habituelles. Pour mémoire, une zone de ségrégation correspond à un découpage fonctionnel du réseau de l'entreprise en régions. Ces régions sont connectées les unes aux autres avec un certain niveau de sécurité. Ce principe est diamétralement opposé à celui de réseau "à plat" ou schématiquement tous les équipements partagent le même réseau physique voire logique.

Cisco recommande donc de scinder le réseau en zones qui sont :

- l'infrastructure qui représente le réseau interne. Ce dernier étant à son tour divisé en trois zones ;
- les filiales ;
- les réseaux longue distance (WAN). Il s'agit des zones d'interconnexions entre l'entreprise et ses filiales via des réseaux de données fournis par des prestataires de télécommunications (fournisseur de service Internet, opérateur Télécom) ;
- la zone DMZ ;
- les zones applicatives ou (Datacenter) qui comprennent les aires de stockage, les centres applicatifs et les services de téléphonie sur IP.

© ENI Editions - All rigths reserved - Moha Anisa

Découpage en zones de sécurité

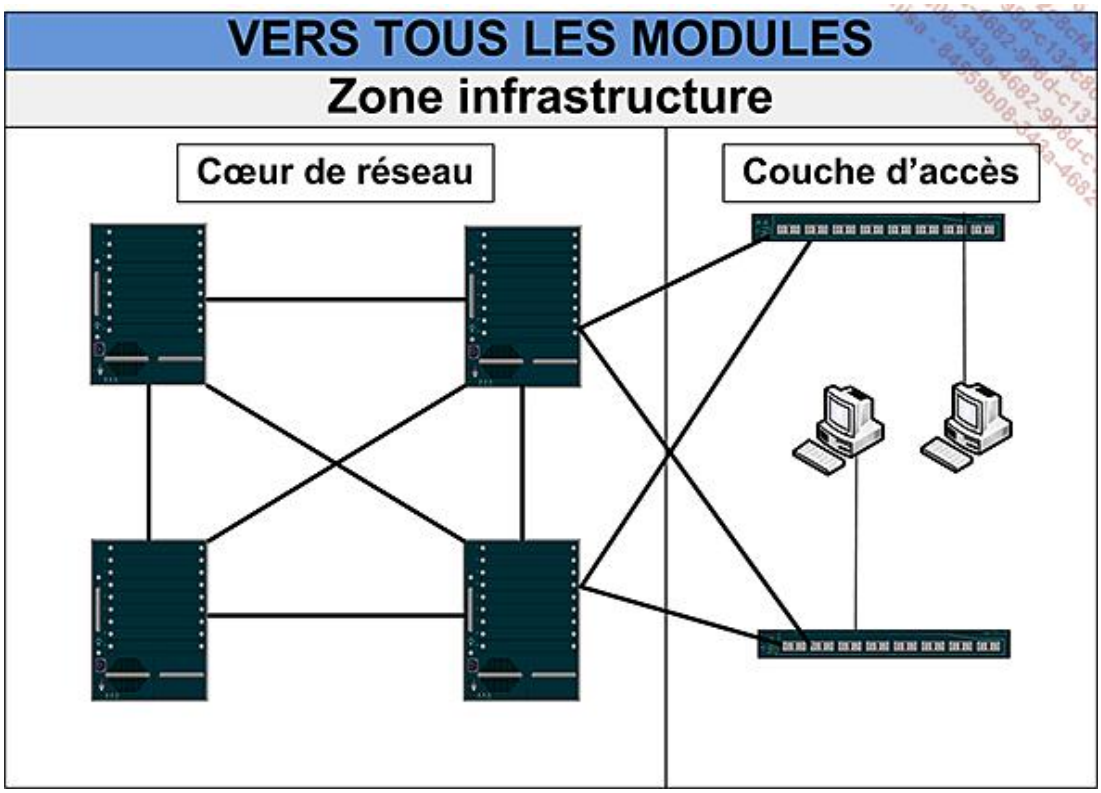
Nous allons donner un aperçu du découpage qui permet d'affecter à chaque zone des fonctions de sécurité basées sur son rôle. Ce découpage fonctionnel facilite considérablement les tâches de surveillance et d'administration en ciblant les mesures de sécurité en fonction de la zone concernée. De plus, chaque zone obtient une certaine indépendance dans sa gestion ce qui ne remet pas en cause la gestion de la sécurité des autres zones qui l'entourent. Toutefois, il faut garder en mémoire que la sécurité d'une zone est étroitement dépendante de celle des zones qui l'entourent.

Quelques règles sont à observer en ce qui concerne la création et l'exploitation des zones de sécurité :

- un équipement ou un hôte qui viendrait à changer de zone doit se conformer aux règles de sécurité de la nouvelle zone. Ceci est du ressort de la sécurité système et vise tout particulièrement les processus de renforcement (*OS Hardening*).

- le trafic ne doit pas transiter entre deux zones dans le sens de la zone la moins sécurisée vers la zone la plus sécurisée.

1. La zone infrastructure



La zone infrastructure est la première des zones de sécurité à considérer car elle est au centre du système d'information. L'étendue de cette zone comprend, dans le cadre de ce livre, le cœur du réseau et la zone d'accès. Les documents publiés par Cisco ont introduit trois zones de base :

- Les zones d'accès sont à l'extrémité du réseau et comprennent les commutateurs sur lesquels sont connectés les postes de travail. Les zones d'accès sont dérivées en deux familles :

    - Les zones dans lesquelles sont fournis des accès filaires.

    - Les zones dans lesquelles sont fournis des accès sans fil.

- Les zones d'agrégation sont constituées par le regroupement des zones d'accès et sont reliées au cœur du réseau avec un niveau de redondance.

- Le cœur de réseau est composé idéalement d'équipements rapides qui relaient le trafic d'une zone à l'autre.

© ENI Editions - All rigths reserved - Moha Anisa

Sur le schéma représentant la zone d'infrastructure, les zones d'accès et d'agrégation sont confondues. Cette architecture est conseillée pour les structures de taille moyenne.

Nous avons décomposé la zone infrastructure en trois sous zones en regard desquelles nous allons faire figurer un groupe d'équipement de sécurité ou de techniques évoquées dans les chapitres précédents.

La zone d'accès est essentiellement sécurisée autour du niveau 2. C'est ici qu'intervient l'authentification obligatoire avant toute possibilité de communiquer. L'implémentation du protocole 802.1X est recommandée. Cette fonction est combinable avec les techniques qui limitent les communications une fois la connexion établie. Citons entre autres les *VACL* et les private *ACL*. Nous avons également à notre disposition toutes les mesures de protection contre les attaques par déni de service ou par usurpation de session que sont *dynamic arp inspection* et *DHCP snooping*.

La zone d'agrégation est située immédiatement à la suite de la zone d'accès à laquelle elle peut être combinée à des fins de simplification. Ici, l'architecture fait intervenir le routage entre les zones d'accès et le reste du réseau avec les limitations imposées par la politique de sécurité. Ce sont donc les techniques de sécurité au niveau 3 qui prévalent comme le filtrage inter *VLAN*, les ACL de tous types et bien sûr la protection des protocoles de routage.

La zone du cœur de réseau ne reçoit pas à proprement parler de fortes mesures de sécurité car, étant au centre de ce dernier, elle bénéficie de la sécurité des zones qui l'entourent. De plus, la rapidité de traitement est de mise au sein de cette zone qui ne saurait souffrir d'aucune latence due à de coûteux contrôles. Malgré tout, la sécurité de cette zone existe. Elle se concentre autour des principes de sécurité des équipements, des protocoles de routage et de la sûreté de fonctionnement grâce aux multiples techniques de redondance.

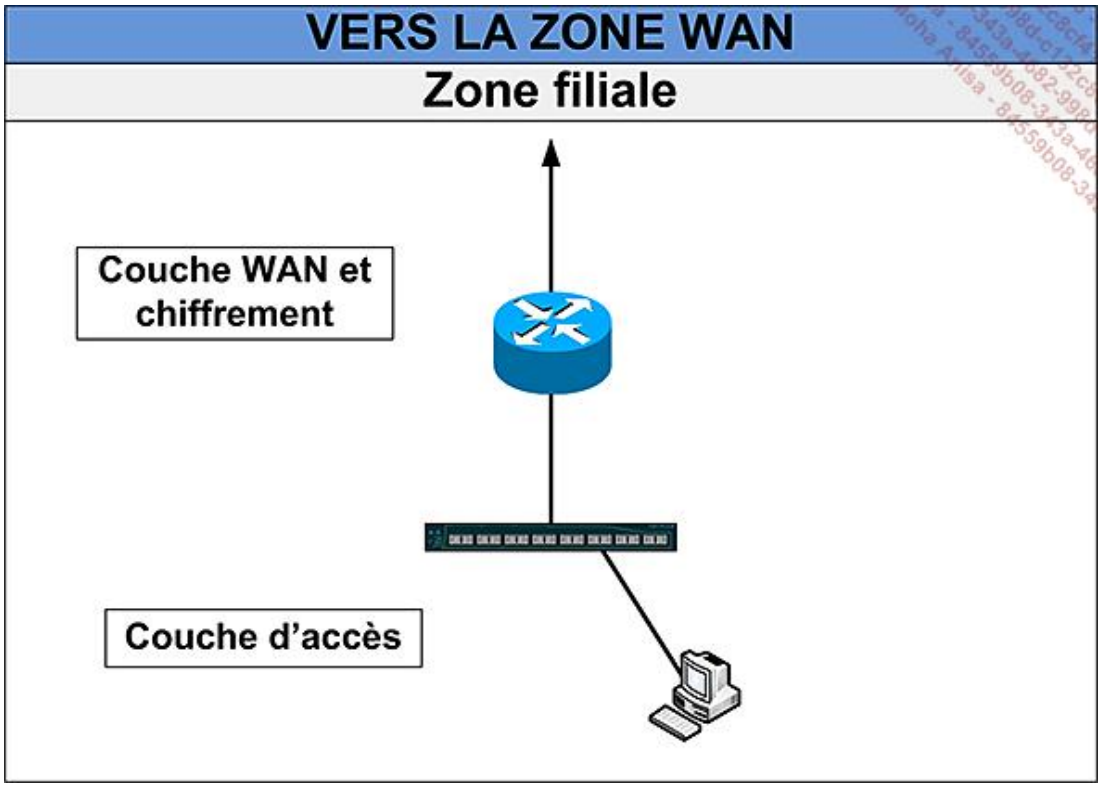
Il va sans dire que la zone d'infrastructure bénéfice d'une sécurité physique renforcée eut égard à son rôle éminemment stratégique. Ici, la moindre interruption de service d'un lien, même prise en charge par la redondance, doit être remise en état le plus rapidement possible. En effet, la défaillance d'un lien bien que prise en compte par un dispositif de secours présente une prise de risque notable en cas de rupture du lien de secours. Ici, il est important de disposer d'un système d'alerte efficace en mesure de détecter tout défaut.

2. Filiales

Une filiale est une zone à part entière de l'entreprise et dispose en règle générale de moyens limités pour assurer sa propre sécurité. Ici, l'efficacité maximale est recherchée avec un nombre réduit d'équipements. La filiale est généralement traitée comme une extension du réseau local et à ce titre bénéficie de tous les services applicatifs. Toutefois, une filiale dispose rarement d'un cœur de réseau à part entière et s'appuie fréquemment sur un unique équipement multifonction qui a pour mission de gérer la sécurité et les connexions vers le site central. La sécurité d'une filiale (considérée comme une extension du réseau local) est sensiblement identique à celle des zones d'accès et d'agrégation. Ici, le protocole 802.1X est chargé d'assurer une stricte authentification des utilisateurs ainsi que la distribution de droits d'accès réseau sous la forme d'ACL reçues après le processus de connexion. Tout comme sur le réseau du site central, le panel des protections de la couche 2 est entièrement disponible pour opérer des séparations entre des zones aux degrés de confidentialité divers.

Les communications de la filiale vers le site central sont habituellement chiffrées. Cette mesure se justifie pleinement si le réseau Internet est voué à cette tâche d'interconnexion. La suite IPSec est tout naturellement indiquée pour accomplir cette tâche entre un équipement de la filiale (mutualisé) et un équipement dédié sur le site central. Bien entendu, des *ACL* opèrent une ségrégation entre le trafic à chiffrer et celui autorisé à transiter en clair. Ceci justifie amplement une étude préalable afin de déterminer les types de trafic à protéger.

© ENI Editions - All rigths reserved - Moha Anisa



Cette notion est importante car les ressources consommées par les processus de chiffrement peuvent se révéler importantes. La zone filiale déploie sur l'équipement de connexion toutes les protections nécessaires vis-à-vis des réseaux extérieurs. Ceci s'applique tout particulièrement si l'Internet est utilisé pour la connexion vers le site central. Nous trouvons ici, les ACL dont le but est de filtrer les *bogon networks* et des mesures visant à limiter les tentatives de connexion frauduleuses utilisées à des fins de saturation.

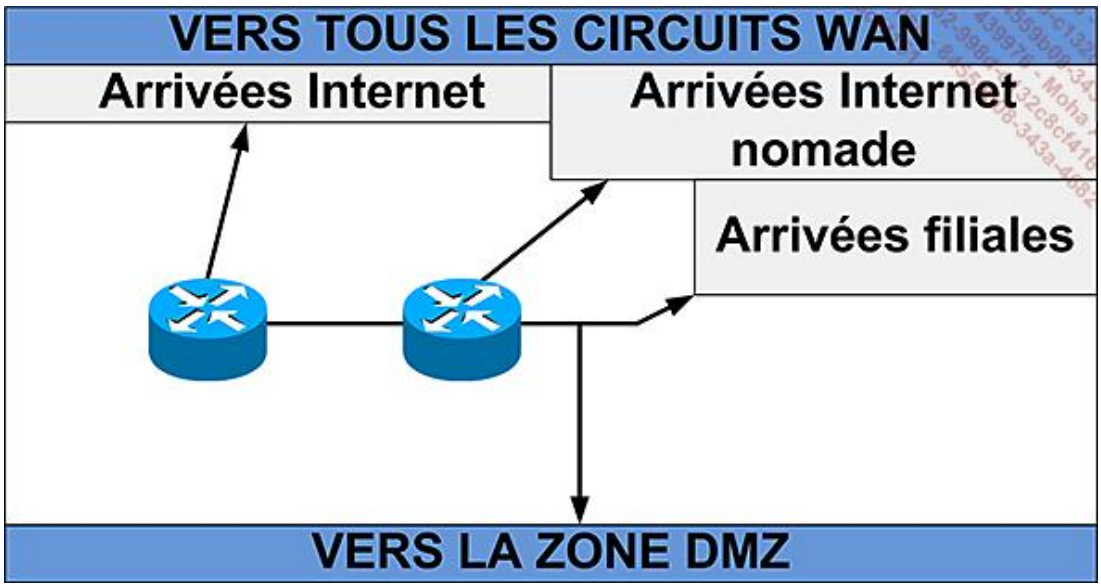
Nous avons abordé au chapitre "La sécurité de la couche réseau" la notion de logon network. Il s'agit de l'ensemble des réseaux IP non attribués sur Internet dont la liste est disponible sur l'URL suivante : www.iana.org/assignments/ipv4-address-space

---

La figure montre une zone filiale relativement simple pour laquelle deux équipements sont en service. Le commutateur Ethernet ainsi que le routeur sont parfois intégrés dans un équipement unique comme le pare-feu *ASA*.

3. WAN

La zone WAN est raccordée aux diverses interfaces qui la relient au monde extérieur.



© ENI Editions - All rigths reserved - Moha Anisa

Ainsi, un sous-réseau est attribué au recueil des collaborateurs nomades, un autre correspond aux arrivées Internet et un dernier est dédié aux filiales. La sécurité sur cette zone comprend les ACL qui écartent du réseau tous les trafics indésirables en provenance d'Internet et la protection logique des équipements. Ces *ACL* reprennent les *bogon networks*. Il est primordial de prendre les mesures de protection visant à limiter certains types de trafic en fonction de leur débit afin de se prémunir contre les attaques par saturation.

Les arrivées des personnels nomades s'effectuent sur les équipements dédiés que sont les concentrateurs VPN ou les pare-feu. Ces derniers embarquent des fonctions de chiffrement de type IPSEC ou SSL. Nous aborderons cette spécificité dans le chapitre consacré aux pare-feu. Chaque arrivée WAN est liée à une politique de sécurité relative aux technologies déployées qui portent par exemple sur la force du chiffrement, l'authentification des utilisateurs et les ACL spécifiques dont héritent les utilisateurs une fois qu'ils sont authentifiés.

La zone WAN assure également le recueil des connexions en provenance des filiales. Les liaisons sont établies sur des lignes louées ou sur Internet. En fonction du type de liaison, les mesures de protection diffèrent. Si la liaison utilise une voie louée, il est important de s'assurer auprès de l'opérateur de télécommunications de la bonne isolation entre le réseau d'interconnexion et les réseaux de l'opérateur voire ceux d'autres clients.

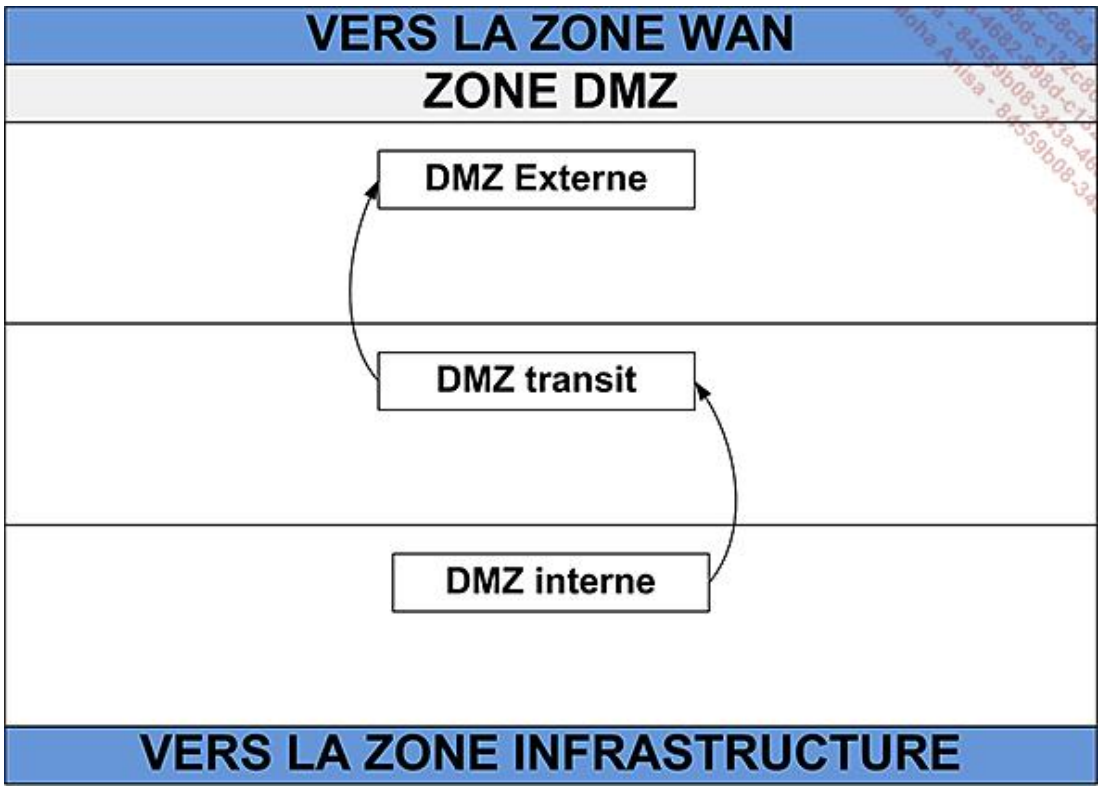
L'entrée de la zone WAN mérite une étroite surveillance des interfaces afin de visualiser toute irrégularité dans le trafic. Un pic ou un creux de trafic indiquent souvent l'imminence d'un problème plus grave.

Les pare-feu et les routeurs sont les principaux intervenants dans la zone WAN. Il est à noter que les deux fonctions peuvent figurer sur le même équipement.

4. La zone DMZ

Les DMZ (*Demilitarized Zones*) sont apparues avec la nécessité de mettre à disposition sur Internet des services applicatifs et de donner accès vers l'extérieur aux personnels de l'entreprise. Si l'on considère la fourniture de service, il est tout à fait inconcevable en terme de sécurité d'autoriser un accès interne à des clients échappant à tout contrôle. Ainsi naquit l'idée de positionner ces services sur une zone déportée formant écran entre le domaine public et le réseau interne de l'entreprise.

Une DMZ est donc une zone tampon située entre ce qui est considéré extérieur et ce qui est considéré intérieur à l'infrastructure centrale. Une DMZ dispose de divers dispositifs de filtrage réseau, mais aussi de relais applicatifs dans le but de ne rien laisser entrer directement au sein de l'infrastructure.



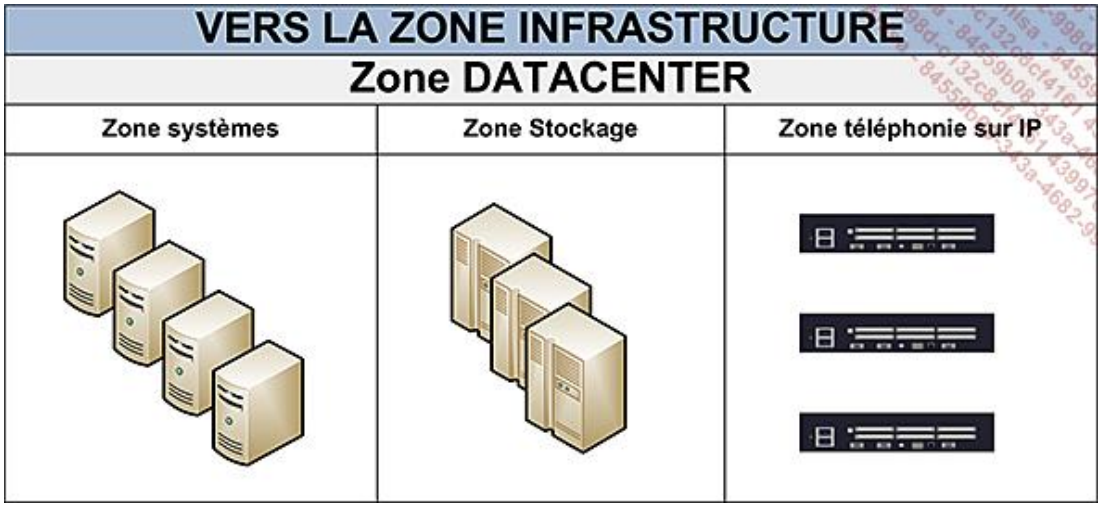
Les DMZ sont connectées par le haut à la zone WAN sur laquelle entrent les connexions en provenance de l'extérieur du réseau et par le bas à la zone d'infrastructure. Le schéma montre trois DMZ organisées comme suit : une DMZ externe, une DMZ de transit et une DMZ interne. Les deux zones d'extrémité hébergent des relais applicatifs (internes ou externes) qui sont habituellement des serveurs de messagerie, des relais HTTP (*web proxies*) et des relais de résolution de nom (DNS). Ces relais possèdent leur propre système de défense. La DMZ de transit quant à elle héberge opportunément des dispositifs de détection d'intrusion et de vérification de code comme par exemple les firewall XML de Cisco car le trafic n'est analysable qu'une fois qu'il est déchiffré. Les zones DMZ peuvent également

© ENI Editions - All rigths reserved - Moha Anisa

héberger des applications autonomes dont les données proviennent de l'intérieur du réseau. Ici s'applique la règle du moindre privilège qui indique que le trafic ne saurait être initialisé d'une zone à faible niveau de sécurité vers une zone dont le niveau de sécurité est plus élevé. C'est pour cette raison que trois flèches sont dessinées sur le schéma, cela indique entre autres que les données présentes dans les DMZ proviennent de l'intérieur du réseau et qu'en aucun cas une entité de la DMZ (un serveur par exemple) ne va de son propre chef rechercher des données à l'intérieur de la zone infrastructure. Des exceptions existent toutefois afin de rendre visible de l'extérieur le réseau d'une entreprise. Il s'agit alors de laisser pénétrer dans les DMZ publiques le trafic en provenance de l'extérieur. Ces dérogations font l'objet de règles de sécurité dans les configurations des équipements et d'une étroite surveillance, elles sont de plus limitées aux premières zones, voire à une seule zone dite publique.

5. La zone Datacenter

La zone Datacenter héberge les serveurs centraux et des baies de stockage de grande capacité. La notion de Datacenter implique une concentration des moyens en un lieu unique dont la sécurité logique est l'une des composantes fortes. Un Datacenter combine en effet toutes les composantes de la sécurité et requiert un niveau de disponibilité à la hauteur de la criticité des informations qu'il héberge. Les mesures de protections associées au Datacenter vont de la protection physique des accès, à la redondance électrique en passant par la protection contre les incendies et la surveillance de la qualité de l'air ambiant pour n'en citer que quelques-unes. L'objectif du Datacenter est avant toute chose, la disponibilité de l'information.



Le Datacenter dispose de sa propre sécurité au niveau des systèmes d'opération et se repose sur la sécurité du réseau pour ne recevoir que des demandes sur les services qu'il offre. À titre d'exemple, une fraction du Datacenter fournissant des services de type http (WEB) attend uniquement des connexions sur le port 80. Celui-ci sera le seul autorisé en entrée sur ladite zone.

La sécurité au niveau réseau du Datacenter repose principalement sur le déploiement d'ACL qui vise à garantir que le trafic entrant autorisé correspond aux services fournis par le Datacenter. Il en va de même en sens inverse en s'assurant de la correspondance du trafic sortant avec les requêtes émises de l'extérieur.

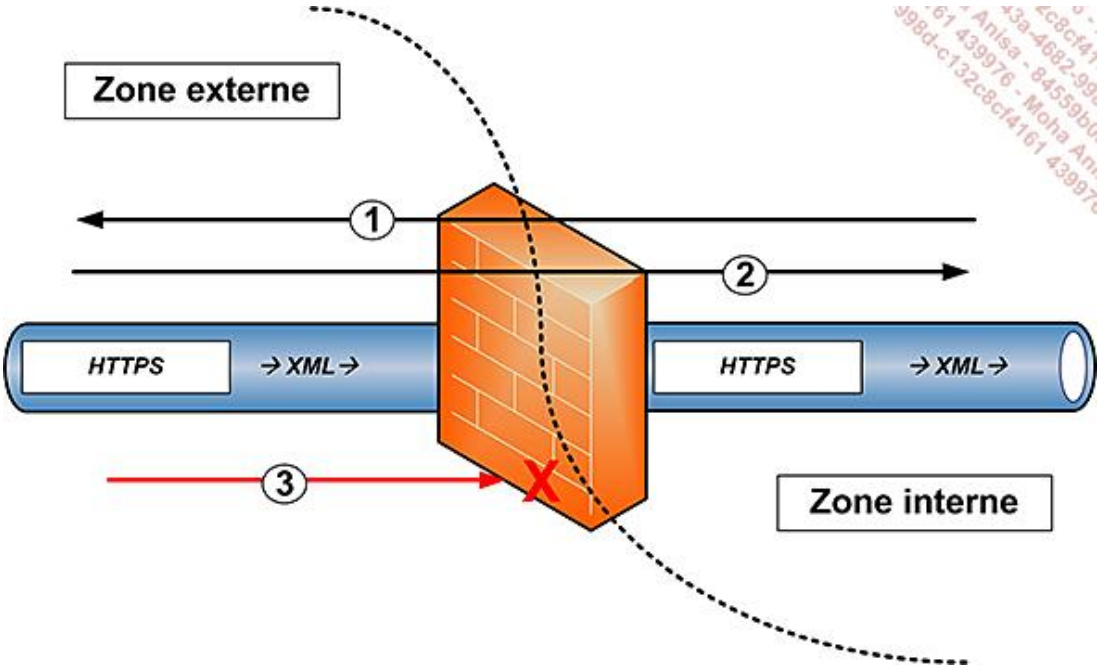
C'est ici aussi la politique de sécurité qui dicte les choix en matière de sens d'initialisation du trafic. Le Datacenter étant une zone interne, le trafic qui y transite n'est habituellement pas chiffré. Cette disposition favorise le déploiement de dispositif d'analyse et de surveillance comme les sondes de détections d'intrusions finement ajustées sur les trafics caractéristiques de la zone. S'il est décidé de chiffrer le trafic, il conviendra de disposer de relais si la surveillance est souhaitée.

Une zone au sein du *datacenter* se démarque, il s'agit de celle qui reçoit les services de téléphonie sur IP. Cette zone est idéalement isolée car la téléphonie est un service hautement stratégique tant par sa confidentialité que par la haute disponibilité qu'il nécessite.

© ENI Editions - All rigths reserved - Moha Anisa

Les pare-feu (Firewalls)

Le ciment entre les diverses zones que nous venons d'examiner est le pare-feu ou firewall en anglais. Les pare-feu ont pour rôle de filtrer le trafic en fonction des informations contenues dans les couches 3 et 4 du modèle OSI. L'évolution des pare-feu vers les modèles conservant l'état des sessions (modèles *stateful*) autorise un suivi du sens d'initialisation des connexions ce qui est très utile entre autres sur le modèle de chaînage des DMZ où chacune possède un niveau de sécurité qui lui est propre. Comme expliqué dans le chapitre sur la sécurité au niveau 3, la politique de sécurité impose que les flux soient toujours initialisés d'une zone dont le niveau de sécurité est élevé vers une zone dont le niveau de sécurité est inférieur. Les contrôles d'état des connexions se charge de laisser entrer les paquets retours venant en réponse aux trafics initiaux.



Ce schéma montre un pare-feu laissant passer les trafics faisant partie d'une session autorisée et bloquant un trafic provenant d'une zone d'un faible niveau de sécurité et tentant de trouver un passage vers l'intérieur du réseau.

Les routeurs Cisco et les commutateurs de niveau 3 sont aptes à remplir le rôle de pare-feu entre les zones conçues par l'architecte de sécurité. Cependant, la limite des pare-feu est flagrante si l'on se place au niveau des couches dites hautes du modèle OSI. En effet un filtrage même avec mémorisation de l'état ne protège aucunement un service contre une attaque purement applicative c'est-à-dire exploitant une faille dans un programme donné. Nous entrons ici dans l'univers des attaques entre autres par injection de code malicieux d'un client vers une application.

Il est devenu indispensable de protéger les applications contre ce type de malveillance qui ne sont pas prise en compte par les firewalls classiques. Le déploiement (pour le protocole http) de relais (*proxies*) et de relais inversés (*reverse-proxies*) dotés de fonctions de sécurité répond parfaitement à cette exigence de filtrage entre les clients et les serveurs. Ces équipements embarquent de nombreux contrôles comme le filtrage d'URL et les scanners anti-virus.

L'insécurité croît aussi avec l'utilisation intensive de la messagerie et des services Web dont les flux transitent entre applications grâce à la souplesse du langage XML embarqué à l'intérieur des protocoles HTTP ou HTTPS. Comme le montre le schéma ci-dessus, les flux 1 et 2 sont gérés par le contrôle d'état et sont autorisés à transiter dans des directions en fonction des règles de sécurité (ACL CBAC). Le flux 3, inconnu est arrêté. Le trafic, bien qu'étant conforme aux règles de sécurité, véhicule potentiellement du code malveillant et l'équipement de filtrage si perfectionné soit-il n'y verra que du feu.

© ENI Editions - All rigths reserved - Moha Anisa

Conclusion

L’architecture de sécurité du réseau est étroitement liée à l’architecture du réseau. Cette imbrication n’est pas sans soulever quelques problèmes lors des évolutions qui ne manquent pas de se produire dans les deux domaines. Les évolutions dans l’un ou l’autre domaine nécessitent une parfaite synchronisation ainsi qu’une parfaite documentation.

Les zones d’architecture que nous venons d’évoquer impliquent une division logique du réseau et le passage d’un réseau dit "à plat" à un réseau hiérarchisé. Ce remaniement s’accompagne opportunément d’une refonte du plan d’adressage IP et d’un renforcement du filtrage entre les zones.

Tout comme la politique de sécurité, l’architecture est en perpétuelle évolution car de nouvelles fonctionnalités et de nouveaux processus viennent enrichir les services dont l’entreprise bénéficie ou qu’elle offre à ses partenaires. Toutes ces ouvertures exposent le système d’information à de nouveaux risques et de nouvelles menaces lesquelles seront traitées pour un renforcement de la sécurité architecturale.

© ENI Editions - All rigths reserved - Moha Anisa

Nécessité de protéger les équipements

Câbles arrachés, alimentations coupées, mots de passe perdus et configurations effacées sont le lot commun de ceux qui ne prêtent aucune attention à la sécurité physique et logique des équipements du réseau.

Les équipements de communication méritent que l'on s'intéresse à eux de près en ce qui concerne la sécurité. Car, si toutes les mesures de protection logiques des couches réseau sont correctement prises, il serait particulièrement gênant de briser la chaîne des flux à cause d'un équipement dont la sécurité intrinsèque aurait été négligée. De plus, les configurations internes des matériels contiennent des éléments hautement confidentiels et révèlent rapidement à un œil exercé une partie de l'architecture du réseau et de sa sécurité.

La nécessité de procéder à une sécurisation rigoureuse d'un routeur ou de tout autre matériel est dès lors toute justifiée.

Une politique de sécurité destinée aux équipements du réseau s'avère nécessaire et doit décrire les exigences ainsi que les procédures d'administration et d'exploitation sécurisées.

Nous allons diviser les exigences de sécurité en trois parties distinctes. La politique qui en découlera comprendra donc également trois parties. Nous allons tout d'abord nous intéresser à la sécurité physique de l'équipement, à sa sécurité logique et à la protection des configurations.

© ENI Editions - All rigths reserved - Moha Anisa

Exigences de sécurité et solutions

1. Physique

Abordons tout d'abord sous forme de tableau les exigences de sécurité physique. Nous mettrons en face de chaque exigence une brève description de la solution avant de la développer.

Exigences de sécurité physique	
Le routeur sera physiquement protégé.	local protégé accès sécurisé par badge avec enregistrement des accès.
Le câblage sera identifiable.	attachement des câbles, état des connecteurs, repérage.
L'alimentation électrique sera garantie.	alimentation redondante.
La température restera dans les normes publiées par le constructeur.	sonde de température dans le local et surveillance des compteurs SNMP sur l'équipement.
La charge CPU et mémoire sera surveillée.	Surveillance des compteurs SNMP.
La charge des liens réseau sera surveillée.	Surveillance des compteurs SNMP.

a. Protection physique

Nous avons déjà abordé cet aspect de la sécurité avec la couche physique du modèle OSI. Toutefois ici, nous entrons dans le domaine de la sécurité des installations informatiques qui vont du simple local technique, à la salle machine en passant par le data center.

Tout équipement se doit de bénéficier d'une protection physique à la hauteur de son coût mais également de son importance au sein du réseau. Les techniques de détection et de lutte contre les incendies dépassent le cadre de ce livre mais sont primordiales et à prendre en compte lors de la construction d'un local à vocation informatique.

La protection physique d'un équipement réseau se traduit par son installation dans un local dont les caractéristiques de protection physique respectent l'état de l'art. Nous parlons ici de contrôle des accès à la salle informatique et de la capacité de ce contrôle à tenir un journal permettant de retracer les entrées et les sorties. Les exigences de sécurité (et donc la politique de sécurité) imposent parfois le recours à une armoire spécifique et sécurisée pour l'accueil des équipements réseau.

Le câblage informatique est un domaine éminemment stratégique et il est très important de disposer d'un inventaire précis et complet indiquant les chemins. Les équipements d'infrastructure du réseau peuvent occuper une place à part entière sur le plan de câblage de l'entreprise. De cette manière lorsque survient un évènement critique, il est plus aisé de définir un chemin alternatif ou de couper des liens si nécessaire. Au niveau de chaque équipement, un repérage méticuleux des câbles rattachés aux équipements s'avère indispensable tout d'abord pour identifier les extrémités dans un même local. Ici, il est opportun de disposer d'une base de données contenant l'ensemble des équipements, leurs connexions et les câbles qui y sont rattachés.

Équipement	**Interface**	**ID Câble**	**Equipement Arr**	**Interface Arr**
Routeur XXX	Interface F x/x	Câble N° YYY	Switch ZZZ	Interface F y/yy

Ce bref exemple montre un exemple d'inventaire de câblage avec lequel il est aisé de retrouver un chemin. Cette technique est aussi valable pour les stations de travail. Les câbles réseaux munis d'étiquettes prénumérotées sont largement disponibles et il existe aussi de nombreux systèmes d'étiquetage industriels permettant d'identifier tous types de câbles (réseaux et électrique).

b. Électricité

Les systèmes d'alimentation électrique à haute disponibilité ne sont pas accessibles à toutes les entreprises. Les systèmes d'alimentation électrique totalement redondants sont coûteux car ils mettent en œuvre des sources alternatives comprenant des séries de batteries et des groupes électrogènes à moteur thermique. L'entretien d'une

© ENI Editions - All rigths reserved - Moha Anisa

telle installation requiert de surcroit une main d'œuvre spécialisée. Les onduleurs, en cas de coupure électrique, fournissent à partir de batteries internes du courant pour une durée définie durant laquelle il est possible d'éteindre le matériel ou d'attendre un retour de l'alimentation. Ces onduleurs sont également capables de remonter en cas de coupure une alarme vers les équipes d'administration.

Si certaines de ces mesures sont tant bien que mal adoptées, il est toutefois primordial de soigner le câblage électrique qui est souvent le parent pauvre. L'expérience et les audits montrent encore trop souvent des montages électriques douteux alimentant des équipements sensibles. Citons brièvement les cascades de prises multiples équipées d'un interrupteur général qui, s'il venait à être actionné couperait irrémédiablement l'alimentation des machines situées en aval. Quant aux câbles proprement dits, étiquetages et fixations solides sont naturellement recommandés.

c. Température

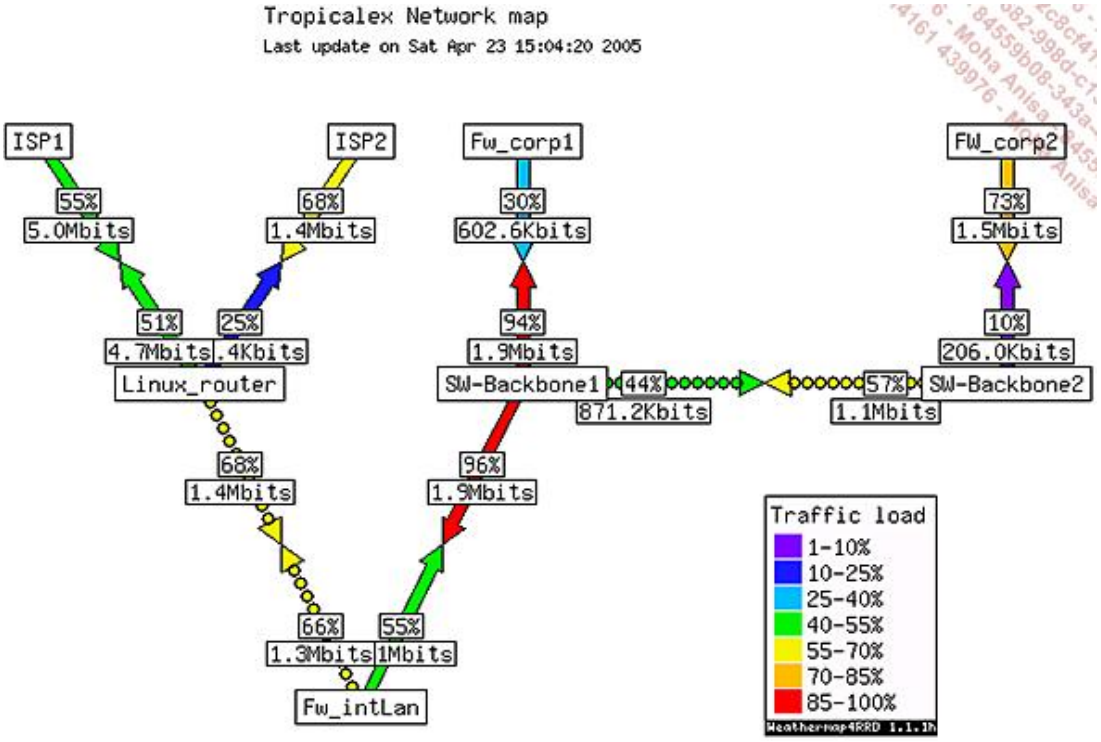
Les équipements du réseau comme tout autre ordinateur sont conçus pour fonctionner dans une plage de température qui est indiquée sur la notice du constructeur. Au-delà ou en deçà de cette plage de température, la bonne marche du système n'est plus garantie. Sur la fiche technique est indiquée la quantité de chaleur émise lors du fonctionnement. Cette quantité est le souvent exprimée en BTU (*British Thermal Unit*). La somme de l'énergie calorifique dégagée indique la puissance de la climatisation qu'il faudra choisir. L'ensemble du dispositif de ventilation est dans la mesure du possible équipé d'un dispositif d'alarme en cas d'approche des seuils indiqués par le constructeur.

d. CPU et Mémoire

Tout comme un ordinateur individuel, un équipement réseau fonctionne avec un processeur et plusieurs types de mémoire qu'il est primordial de surveiller. À l'instar de la température, une augmentation (tendant vers la limite publiée) de la consommation de mémoire ou de processeur indique un dysfonctionnement en cours ou à venir. Afin de surveiller les compteurs d'utilisation, l'activation du protocole SNMP est toute indiquée en respectant les précautions d'usage en matière de sécurité.

e. Charge des liens réseau

Les interfaces physiques ou virtuelles d'un routeur par exemple sont en permanence soumises à une certaine charge de trafic. En fonction des heures du jour et de la nuit, d'une période particulière de l'année, voire d'un évènement. Comme la température, les compteurs mémoire et CPU, la charge de trafic est une indication particulièrement intéressante sous plusieurs aspects. Tout d'abord elle indique si le réseau reçoit du trafic et si tel est le cas il devient possible d'observer l'activité en temps réel. Une telle surveillance si elle est de plus couplée avec un système d'alarme en cas de dépassement de seuil permet de détecter par exemple une montée en charge inhabituelle. Des logiciels libres et très performants s'acquittent de ces tâches en offrant de surcroît d'intéressantes fonctions d'historique dont l'analyse permet d'anticiper les redimensionnements futurs du réseau.



© ENI Editions - All rigths reserved - Moha Anisa

Voici un exemple d'un écran de surveillance du pourcentage d'occupation des liens d'un réseau. Le logiciel utilisé est Weathermap 4 RRD. Les couleurs des flèches donnent rapidement une tendance de l'utilisation des interfaces surveillées. Ce logiciel exploite une base RRD qui permet de conserver un historique du trafic.

RRD tool (*Round Robin Database*) est un logiciel libre d'une grande puissance qui permet de générer des graphes. Il est disponible ici : http://oss.oetiker.ch/rrdtool/

2. Sécurité logique

La sécurité logique des équipements réseau concerne principalement la protection des accès à la console ou au serveur Web embarqué. Cisco a muni ses produits d'interfaces physiques et logiques afin qu'un administrateur puisse se connecter et accéder à la ligne de commande.

Tout comme pour la sécurité physique, il nous faut en premier lieu exprimer les exigences de sécurité.

Exigences de sécurité logique	
Temps synchronisé avec authentification de la source.	Protocole NTP avec authentification MD5.
Protection des accès via les ports série et auxiliaire.	Authentification par compte local ou externe.
Enregistrement des tentatives d'accès.	Commandes `login on-failure`, `login on-success`.
Contrer les tentatives de découverte d'un compte.	Commande `login block-for`.
Authentification et chiffrement des accès.	Protocole SSH version 2.
Limiter le temps d'inactivité.	Commande `exec-timeout`.
Limiter l'accès à certaines commandes et informations.	Accès à la ligne de commande basé sur des rôles.
Protéger les informations émises par le routeur.	Chiffrement des messages SYSLOG et SNMP.

a. À la bonne heure

Les informations générées par SYSLOG ne sont pas véritablement exploitables tant qu'elles ne sont pas estampillées avec l'heure à laquelle l'évènement s'est produit. C'est pour cette raison qu'il est indispensable de régler l'heure d'un équipement avant sa mise en exploitation. Il est recommandé pour ce faire d'utiliser les services d'un serveur de temps connu aussi sous la désignation de serveur NTP (*Network Time Protocol*). Rien de plus simple avec un routeur Cisco, il suffit d'entrer la commande suivante :

```
R0(config)#ntp server 192.168.0.38
```

```
R0#sh ntp status
Clock is synchronized, stratum 2, reference is 192.168.0.38
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision
is 2**18
reference time is CC7651DA.62FA027C (14:51:06.386 UTC Sat Sep 13
2008)
clock offset is -8.7854 msec, root delay is 36.13 msec
root dispersion is 14.43 msec, peer dispersion is 5.63 msec
```

Voici le résultat de la commande `show ntp status` montrant la synchronisation de l'heure du routeur avec le serveur de temps.

Mais, dans un souci évident de sécurité, pouvons-nous faire confiance aux informations provenant du serveur de temps configuré ici ? Rien n'est moins sûr et il faut recourir une nouvelle fois à un protocole offrant un système d'authentification.

```
R0(config)#ntp authenticate
R0(config)#ntp authentication-key 1 md5 cisco
```

© ENI Editions - All rigths reserved - Moha Anisa

```
R0(config)#ntp trusted-key ?
  <1-4294967295>  Key number

R0(config)#ntp trusted-key 1
R0(config)#ntp server 192.168.0.38 key 1
R0(config)#ntp access-group peer 10
```

Tout d'abord, l'authentification est activée. Puis une clé portant le numéro 1 est créée. Cette clé sera protégée en md5. La commande `trusted-key` désigne cette clé comme étant une clé valide. La commande dans laquelle se trouve l'adresse IP du routeur associe celui-ci avec la clé numéro 1. Pour terminer, une ACL est appliquée aux requêtes NTP.

Une fois l'équipement synchronisé, les deux commandes suivantes permettent d'estampiller avec l'heure et la date les évènements SYSLOG et les messages issus des commandes de l'outil de diagnostic `debug`.

```
R0(config)#service timestamps log datetime localtime year
R0(config)#service timestamps debug datetime localtime year
```

b. Ports Console et Auxiliaire

Examinons tout d'abord les connecteurs externes. Nous trouvons sur un routeur un port Console et un port Auxiliaire.

Le port console se présente sous la forme d'un connecteur DB9 ou de type RJ45. Un câble connecté à ce port et au port série d'un PC (COM1) donne accès à la ligne de commande du routeur via une interface généralement nommée *con 0*.

L'accès à la ligne de commande via cette interface ne souffre d'aucune dérogation en matière de sécurité. Il est possible de protéger la connexion selon deux méthodes : le mot de passe enable ou un compte d'utilisateur.

- La première méthode donne accès dans un premier temps au mode non privilégié. Il est alors nécessaire d'entrer le mot de passe *enable* pour accéder au mode privilégié.

- La seconde méthode est plus sécurisée que la première et requiert la création d'un compte local. Ce compte est alors requis lors de la connexion à condition toutefois d'avoir configuré l'interface *con 0* en ce sens.

```
R0(config)#username vincent password cisco

R0(config)#line con 0
R0(config-line)#login local
```

La première ligne crée un compte local à l'équipement. La troisième ligne impose aux connexions entrantes via le port console une authentification avec la base de compte locale du routeur.

Cette interface est très pratique lorsque l'équipement doit être dépanné et qu'il est inaccessible par le réseau. Afin de faciliter les opérations en cas d'urgence, il est recommandé de laisser le câble de la console à côté de l'équipement.

Le port AUX (auxiliaire) du type DB 25 ou RJ 45 est utilisé pour connecter un modem au routeur afin de le rendre accessible par l'intermédiaire d'une ligne téléphonique analogique. Une fois connecté, il est nécessaire de s'authentifier tout comme pour le port console.

Il est primordial de tracer les tentatives de connexions réussies ou se soldant par un échec. Deux commandes existent pour satisfaire à cette exigence :

```
R0(config)#login on-failure log
R0(config)#login on-success log
```

Ici, les tentatives couronnées de succès et infructueuses sont enregistrées via le service SYSLOG.

Tout équipement peut être victime d'une attaque visant à découvrir un compte valable. Il est possible de limiter dans le temps ces tentatives en introduisant un délai entre elles.

```
R0(config)#login block-for 120 attempts 3 within 10
```

Ici, le routeur refusera toute tentative durant deux minutes (120s) s'il a précédemment reçu plus de trois tentatives d'accès (sans succès) en moins de dix secondes.

c. Telnet et SSH

© ENI Editions - All rigths reserved - Moha Anisa

Telnet est un protocole client serveur qui nous semble provenir du fond des âges tant il est intégré dans les ordinateurs au point que son nom est entré dans le langage courant. Basé sur TCP/IP, Telnet rend d'innombrables services de par le monde et son côté pratique a largement contribué à sa distribution et à sa popularité. Toutefois, Telnet présente en terme de sécurité de très nombreux désavantages comme celui de ne pas chiffrer les communications. Ainsi, la séquence d'authentification entre le client et le serveur passant en clair sur le réseau révèle directement le mot de passe de l'utilisateur qui tente de se connecter.

Un routeur Cisco implémente par défaut un service Telnet qui est disponible sur les interfaces virtuelle VTY (*Virtual Terminal*). Il est malgré tout indispensable d'avoir entré un mot de passe dans la configuration ou de faire appel au service d'authentification. Tout ceci reste cependant insuffisant au regard des menaces actuelles qui planent sur les réseaux.

La protection des accès (via le réseau) à la ligne de commande est une nécessité et ce fait est universellement reconnu. C'est la raison pour laquelle le protocole SSH connait depuis quelques années un franc succès.

L'implémentation du protocole SSH (*Secure Shell*) sur les produits Cisco offre la possibilité de se connecter en toute sécurité à un hôte distant en chiffrant toute la communication y compris la séquence d'authentification. Cisco fournit également un client SSH en remplacement du client Telnet. Il est à noter que SSH nécessite une version d'IOS fournissant les services de chiffrement.

Observons la configuration de SSH sur un routeur ainsi qu'une tentative de connexion.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#host R0
R0(config)# ip domain name TestLab.fr

R0(config)#crypto key generate rsa modulus 2048
The name for the keys will be: R0.TestLab.fr

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R0(config)#
*Mar  1 00:06:38.919: %SSH-5-ENABLED: SSH 1.99 has been enabled

R0(config)# ip ssh version 2
```

En mode de configuration il suffit :

- de donner un nom d'hôte au routeur et un nom de domaine dans un premier temps ;
- de générer une paire de clés de type RSA. Un modulo de 2048 bits est requis ici. La politique de sécurité relative au chiffrement indique la complexité requise pour le modulo.
- de lancer SSH dans sa version 2. Pour mémoire, le retour mentionnant SSH 1.99 renseigne sur la possibilité d'utiliser SSH version 1 ce qui n'est pas recommandé pour des raisons de sécurité.

```
R0(config)#line vty 0 4
R0(config-line)#transport input ssh
R0(config-line)#login local
R0(config-line)#exec-timeout 0 30
R0(config)#access-class 10 in
R0(config-line)#exit
R0(config)#username vincent password cisco
R0(config)#service password-encryption
R0(config)#enable secret cisco
```

Les lignes suivantes se passent de commentaires si le lecteur est familier de la configuration des équipements Cisco. Cependant, une commande est ici importante. Il s'agit de `transport input ssh` qui oblige la connexion distante à utiliser SSH.

La commande `exec-timeout 0 30` est primordiale car elle permet de ne pas laisser la console connectée en cas d'inactivité de l'utilisateur. Le premier chiffre (ici 0) représente les minutes et le second (ici 30) représente les secondes. Dans le cas exposé, l'utilisateur sera déconnecté après 30 secondes d'inactivité.

Pour mémoire, nous créons un utilisateur local et nous activons le service de chiffrement des mots de passe.

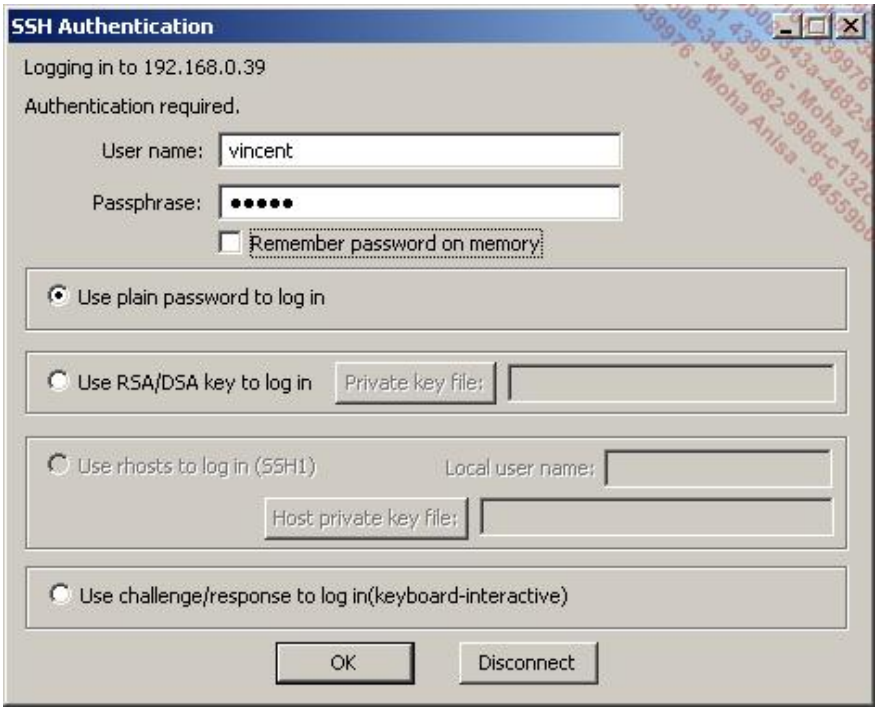
En fonction des versions il est parfois nécessaire pour activer SSH d'entrer la commande : `aaa new-model`.

© ENI Editions - All rigths reserved - Moha Anisa

Ne pas oublier de positionner une ACL pour donner la touche finale à la protection des accès via SSH avec la commande : `access-class 10 in`.

SECURITY WARNING
There is no entry for the server "192.168.0.39" in your list of known hosts. The machine you have contacted may be a hostile machine pretending to be the server.
If you choose to add this machine to the known hosts list and continue, then you will not receive this warning again.
The server's host key fingerprint is:
bb:09:73:de:0a:00:48:06:21:0d:1b:fb:03:31:5e:19
Add this machine and its key to the known hosts list
Continue
Disconnect

Lors de la première connexion, un écran de ce type apparaît et demande à l'utilisateur de valider l'empreinte de la clé publique du serveur. Il est important qu'un utilisateur distant connaisse au préalable cette empreinte. Dès lors, à la réception de cet écran l'utilisateur sera en mesure de la valider avec celle qu'il possède déjà. Dans le cas contraire, l'utilisateur s'expose au risque de subir une attaque du type « man in the middle » c'est-à-dire de se voir présenter une clé appartenant à une personne malveillante.



Voici l'écran qui précède la connexion. À noter, il est demandé au client SSH de ne pas mémoriser le mot de passe en mémoire. Cette mesure est applicable à tous les clients quels qu'ils soient.

Nous venons de montrer que l'implémentation du protocole SSH est excessivement simple. Il est toutefois nécessaire de posséder un routeur disposant des fonctions de chiffrement ce qui occasionne un coût supplémentaire.

d. SNMP et SYSLOG

SNMP

SNMP ou *Simple Network Management Protocol* assure en mode client-serveur l'envoi de messages entre l'équipement sur lequel réside l'agent SNMP et un serveur qui interroge celui-ci. L'agent SNMP est aussi capable d'émettre de lui-même des messages à destination du serveur. Ces messages portent le nom de trap. Il existe trois versions du protocole SNMP qui se différencient les unes des autres par le niveau de sécurité offert. Seule la version 3 permet le

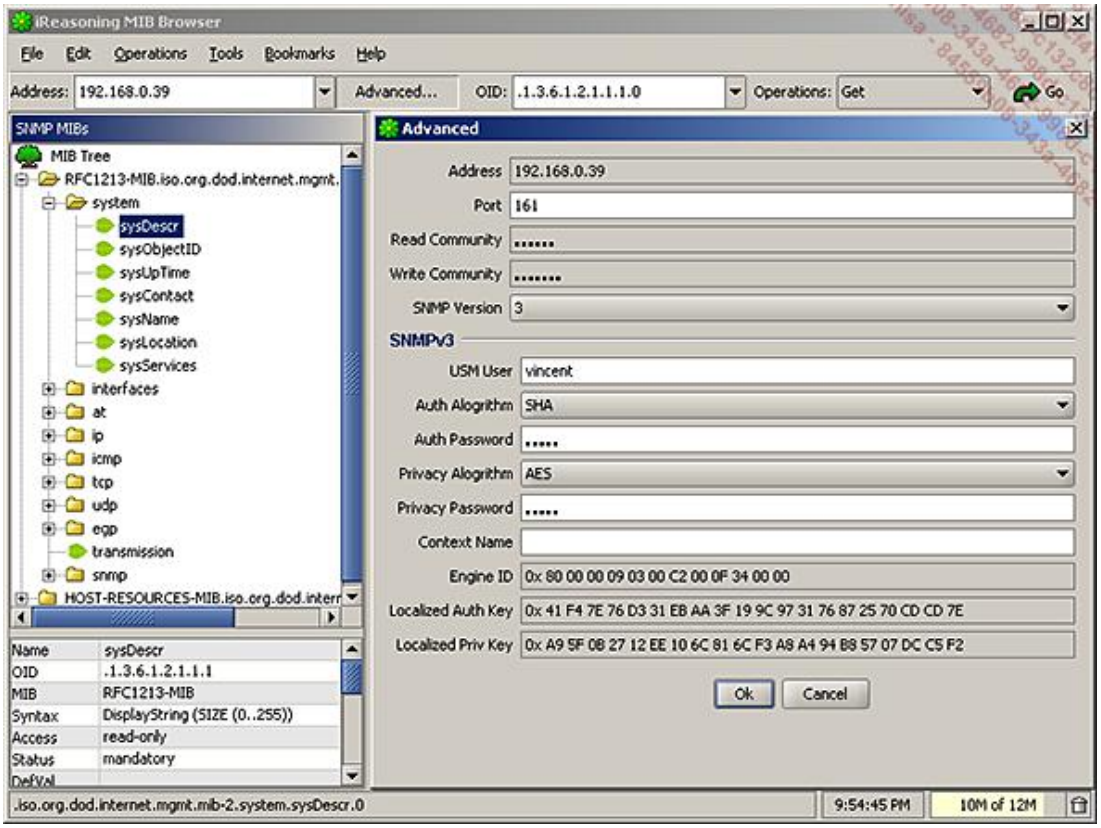
© ENI Editions - All rigths reserved - Moha Anisa

chiffrement et l'authentification des messages. Cette version est à privilégier dans les environnements hautement sécurisés. Examinons un exemple de configuration.

```
R0(config)# snmp-server group TESTLAB v3 priv access 10
R0(config)# snmp-server user vincent TESTLAB v3 auth sha cisco priv
aes 128 cisco access 10
```

Ces deux commandes sont assez complexes et sont associées l'une à l'autre avec le mot TESTLAB. La première commande définit un groupe nommé TESTLAB qui utilise la version 3 du protocole SNMP. Le mot priv spécifie l'authentification et le chiffrement des messages. L'ACL 10 est appliquée pour filtrer l'adresse source des requêtes.

La seconde commande déclare l'utilisateur vincent dans le groupe TESTLAB. La version 3 de SNMP est utilisée avec une authentification basée sur les protocoles SHA et chiffrée en aes 128. L'access-list 10 est également appliquée.



Voici un client SNMP sur le point d'interroger l'agent SNMP de l'équipement afin d'obtenir la description du système.

```
Sep 13 2008 20:03:05: SNMP: Packet received via UDP from
192.168.0.38 on FastEthernet0/0

Sep 13 2008 20:03:05: SNMP: Get request

R0(config)#, reqid 59802776, errstat 0, erridx 0
 system.1.0 = NULL TYPE/VALUE
Sep 13 2008 20:03:05:

Incoming SNMP packet
Sep 13 2008 20:03:05: v3 packet security model: v3 security level:
priv

Sep 13 2008 20:03:05: username: vincent
Sep 13 2008 20:03:05: snmpEngineID: 800000090300C2000F340000
Sep 13 2008 20:03:05: snmpEngineBoots: 1      snmpEngineTime: 2633

Sep 13 2008 20:03:05: SNMP: Response, reqid 59802776, errstat 0,
erridx 0
 system.1.0 = Cisco IOS Software, 3700 Software (C3725-
ADVSECURITYK9-M), Version 12.4(11)XW5, RELEASE SOFTWARE (fc1)

Sep 13 2008 20:03:05: SNMP: Packet sent via UDP to 192.168.0.38
```

© ENI Editions - All rigths reserved - Moha Anisa

Nous observons dans les retours des commandes `debug snmp packets` et `debug snmp headers`, l'arrivée du paquet SNMP, le type d'authentification et la réponse envoyée par l'agent SNMP du routeur vers le client SNMP.

Le protocole SNMP facilite la surveillance de très nombreux paramètres parmi lesquels l'activité des interfaces réseau. Les outils de mesure d'occupation des liens effectuent une simple soustraction entre deux valeurs des compteurs *ifinoctets* (trafic entrant en Octets) et une division par l'intervalle de temps entre les deux mesures.

SYSLOG

Le protocole SYSLOG est sans doute contemporain de Telnet. De plus, il est tout comme lui efficace ce qui l'a rendu populaire et indispensable. SYSLOG se propose d'envoyer sur le réseau les messages issus d'évènements générés par un système d'exploitation. Les messages SYSLOG sont clairement visibles lorsque l'on quitte le mode de configuration pour revenir en mode *exec* avec la commande end (ou la séquence simultanées des touches [Ctrl] **Z**).

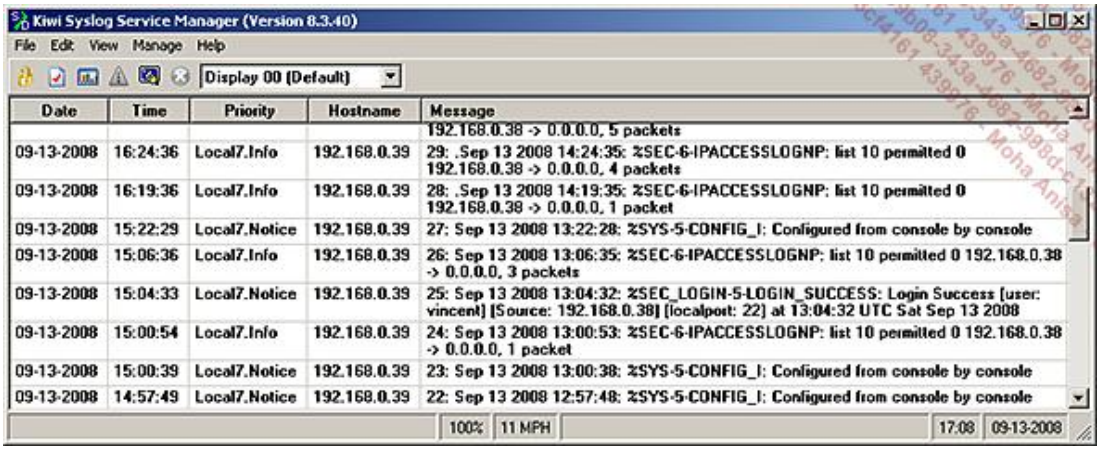
```
R0(config)#logging on
R0(config)#logging console ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  discriminator  Establish MD-Console association
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  guaranteed     Guarantee console messages
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
```

Les messages issus du système sont visibles sur la console qui est disponible directement sur le port du même nom (Con0 dans la configuration) ou sur une session distante (Telnet ou SSH) avec la commande `terminal monitor`.

Tout d'abord, il est indispensable de passer la commande `logging on` afin d'activer globalement le service, puis de signifier au système les types de messages à renvoyer vers la console. La commande `logging console 6` dirigera vers la console les messages système d'une `severity de 6` jusqu'à `0` ignorant les messages de niveau `7`.

```
R0(config)#logging on
R0(config)#logging host 192.168.0.38
```

Cette séquence de commandes dirige tous les messages vers un serveur SYSLOG externe comme celui proposé par la société *KIWI entreprise*.


Kiwi Syslog Service Manager (Version 8.3.40)
File Edit View Manage Help
Display 00 (Default)
Date Time Priority Hostname Message
09-13-2008 16:24:36 Local7.Info 192.168.0.39 29: .Sep 13 2008 14:24:35: %SEC-6-IPACCESSLOGNP: list 10 permitted 0 192.168.0.38 -> 0.0.0.0, 4 packets
09-13-2008 16:19:36 Local7.Info 192.168.0.39 28: .Sep 13 2008 14:19:35: %SEC-6-IPACCESSLOGNP: list 10 permitted 0 192.168.0.38 -> 0.0.0.0, 1 packet
09-13-2008 15:22:29 Local7.Notice 192.168.0.39 27: Sep 13 2008 13:22:28: %SYS-5-CONFIG_I: Configured from console by console
09-13-2008 15:06:36 Local7.Info 192.168.0.39 26: Sep 13 2008 13:06:35: %SEC-6-IPACCESSLOGNP: list 10 permitted 0 192.168.0.38 -> 0.0.0.0, 3 packets
09-13-2008 15:04:33 Local7.Notice 192.168.0.39 25: Sep 13 2008 13:04:32: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: vincent] [Source: 192.168.0.38] [localport: 22] at 13:04:32 UTC Sat Sep 13 2008
09-13-2008 15:00:54 Local7.Info 192.168.0.39 24: Sep 13 2008 13:00:53: %SEC-6-IPACCESSLOGNP: list 10 permitted 0 192.168.0.38 -> 0.0.0.0, 1 packet
09-13-2008 15:00:39 Local7.Notice 192.168.0.39 23: Sep 13 2008 13:00:38: %SYS-5-CONFIG_I: Configured from console by console
09-13-2008 14:57:49 Local7.Notice 192.168.0.39 22: Sep 13 2008 12:57:48: %SYS-5-CONFIG_I: Configured from console by console
100% 11 MPH 17:08 09-13-2008

Voici, présentés dans le logiciel *Kiwi Syslog manager*, les messages issus d'un routeur. Nous y trouvons pêle-mêle des informations relatives à des accès, des modifications de la configuration ou encore des messages provenant d'ACL à la fin desquelles se trouve le mot `log`.

Si les retours de SYSLOG sont renvoyés vers la console avec la commande `logging console` un problème de sécurité se pose en cas d'échec d'authentification si cette dernière est effectuée sur le port console (con 0). En effet, le message indique si le rejet est du à une erreur de nom d'utilisateur ou du mot de passe. Ces informations sont autant d'indications fournies à une personne malveillante dans sa quête d'un accès comme le montre le code suivant.

```
Username: vincent
Password:
```


© ENI Editions - All rigths reserved - Moha Anisa

```
% Login invalid

Username:
Sep 13 2008 20:33:44: %SEC_LOGIN-4-LOGIN_FAILED: Login failed
[user: vincent] [Source: 0.0.0.0] [localport: 0] [Reason: Login
Authentication Failed - BadPassword] at 20:33:44 UTC Sat Sep 13
2008
Username:
```

Ici, nous savons que le nom d'utilisateur est correct mais que le mot de passe est erroné. Nous sommes donc en possession de la moitié de la séquence d'authentification. Il est donc recommandé de désactiver la commande `logging console`.

e. Rôles administratifs

Il est souhaitable dans une entreprise ayant à gérer un parc d'équipement conséquent de disposer d'une politique d'accès aux diverses fonctionnalités des équipements. Il est possible de créer des rôles dans le but de donner à chacun d'eux l'accès à un ensemble limité de fonctions. Ainsi, la confidentialité de la configuration du routeur et la répartition des responsabilités s'en trouvent améliorées.

Dans la terminologie utilisée par Cisco, le terme de vue (view) est employé. Il en existe deux types :

- La vue *root* qui dispose de tous les privilèges dont celui de créer d'autres vues.
- Les vues liées à un rôle qui disposent de tout le panel des commandes existantes sur l'équipement.

Avant toute chose, il est indispensable d'activer AAA avec la commande `aaa new-model` puis de se déconnecter du mode privilégié avant de configurer l'équipement suivant l'exemple suivant.

```
R0>enable view
Password:

R0#
*Mar  1 02:42:51.331: %PARSER-6-VIEW_SWITCH: successfully set to
view 'root'.
```

La première commande suivie du mot de passe *enable* permet d'entrer dans la vue *root* à partir de laquelle nous allons paramétrer les autres vues.

```
R0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#parser view admin-reseau
R0(config-view)#
```

La vue portant le nom *admin-reseau* est créée à partir de la vue *root*.

```
R0(config-view)# secret 0 cisco
R0(config-view)# commands configure include all interface
R0(config-view)# commands exec include traceroute
R0(config-view)# commands exec include ping
R0(config-view)# commands exec include configure terminal
R0(config-view)# commands exec include configure
R0(config-view)# commands exec include all show ip
```

À cette vue sont ajoutées les commandes jugées nécessaires pour ce rôle d'administration. Le mot de passe secret de cette vue sera naturellement chiffré par le système.

```
R0>enable view admin-reseau
Password:

R0#
*Mar  1 02:58:17.631: %PARSER-6-VIEW_SWITCH: successfully set to
view 'admin-reseau'.

R0#?
Exec commands:
  configure   Enter configuration mode
  enable      Turn on privileged commands
```

© ENI Editions - All rigths reserved - Moha Anisa

```
  exit        Exit from the EXEC
  ping        Send echo messages
  show        Show running system information
  traceroute  Trace route to destination

R0#sh
R0#show ?
  ip  IP information
```

Pour accéder au rôle, il faut tout d'abord entrer la commande `enable view` suivie du nom de la vue. Le message SYSLOG indique que nous sommes entrés dans cette vue avec succès. En entrant le point d'interrogation seul nous observons toutes les commandes disponibles dans le mode *Exec*. Nous pouvons aussi examiner les options disponibles après la commande `show`. Dans notre cas, seules les commandes commençant par `show ip` sont disponibles.

```
R0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#?
Configure commands:
  do         To run exec commands in config mode
  exit       Exit from configure mode
  interface  Select an interface to configure
```

Ici, nous procédons à la verification du mode de configuration. Comme prévu, seul le mode de configuration des interfaces est proposé.

f. Protection des données émises

La politique de sécurité impose parfois de protéger les informations issues de l'équipement en fonction du type de liaison (locale ou distante) et du type de réseau (privé ou public). Nous venons d'examiner les protocoles SYSLOG et SNMP qui entrent dans ce cas de figure. Les informations émises par ces deux services transportent l'état physique et logique de l'appareil lors de son fonctionnement. Il est donc primordial d'assurer un transit sécurisé de ces états afin qu'ils ne soient ni interceptés et encore moins modifiés sur le trajet entre l'équipement et le serveur chargé de réceptionner les données. En cas de litige la protection des informations durant le transit en assurant l'intégrité du message et notamment la correspondance entre l'évènement et son heure d'occurrence.

Le protocole IPSec est tout naturellement désigné pour accomplir cette tâche. Nous avons examiné sa configuration dans un chapitre précédent. La protection des données issues des services SNMP et SYSLOG consiste donc à créer une crypto-map entre le routeur et le serveur accueillant les messages. Les services IPSec sont disponibles sur les plates-formes Microsoft et Linux. Soulignons aussi l'opportunité de filtrer ces communications vers les serveurs de destination à l'aide d'ACL appropriées.

3. Sécurité des configurations et du système d'exploitation

Des informations sensibles sont présentes dans la configuration d'un équipement réseau. Citons entre autre les mots de passe des utilisateurs locaux et clés de chiffrement IPSec. Le système d'exploitation est lui aussi au centre de toutes les attentions. Présentons comme à l'accoutumée les exigences de sécurité.

Exigences de sécurité des configurations et du système d'exploitation	
Ne pas installer une image IOS corrompue.	Utilisation de MD5.
Protéger les mots de passe dans le fichier de configuration.	Chiffrement des mots de passe.
Protection des clés de chiffrement.	Chiffrement des clés dans la configuration.

a. Sécurité de l'image du logiciel IOS

Le système d'exploitation d'un routeur Cisco se nomme IOS (*Internetwork Operating System*) et ce logiciel n'est pas exempt de défauts tant ses possibilités sont étendues. Ces imperfections (on parle de bug) ont parfois un impact direct sur la sécurité de l'équipement et par extension sur le réseau tout entier. La politique de sécurité impose généralement de surveiller les vulnérabilités et d'appliquer les correctifs qui s'imposent en respectant toutefois une certaine procédure. Les entreprises ne sont pas toutes égales face aux menaces informatiques et ceci est principalement dû au manque de moyen dans les fonctions de sécurité et plus particulièrement en matière de

© ENI Editions - All rigths reserved - Moha Anisa

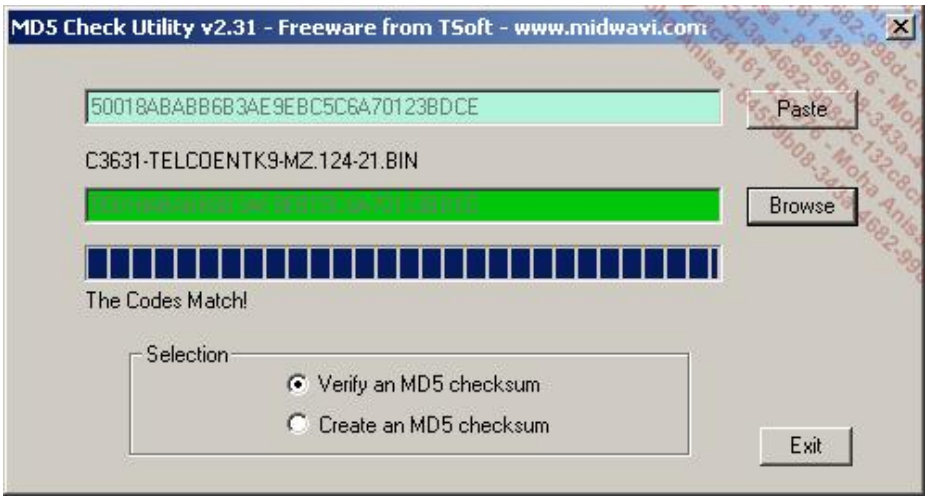
surveillance des vulnérabilités impactant le parc informatique.

Concernant le système d'exploitation IOS, il est fortement recommandé de suivre les publications de vulnérabilités le concernant et de prendre les bonnes décisions en fonction des impacts potentiel sur le réseau voire le système d'information tout entier. Les changements de versions nécessitent l'application de procédures relativement simples mais incontournables. Elles consistent principalement à appliquer la nouvelle version sur un équipement représentatif de ceux se trouvant en cours d'exploitation. Si aucun équipement représentatif n'est disponible, une fenêtre d'intervention sera négociée afin de procéder au changement de version sur un équipement en cours d'exploitation. Cette fenêtre sera planifiée en tenant compte du temps nécessaire pour effectuer un éventuel retour en arrière. Bien entendu la configuration et l'IOS en cours seront sauvegardés. Préalablement à toute installation d'un nouvel IOS sur un équipement, il faut le télécharger sur le site Internet de Cisco ou se le procurer auprès de son fournisseur. Afin d'éviter une corruption du logiciel (on parle aussi d'image) une vérification s'impose et consiste à vérifier l'empreinte MD5 de l'IOS. Voici comment procéder.

Tout d'abord, le site web de Cisco fournit une empreinte MD5 de l'image que l'on est sur le point de télécharger. Une fois l'IOS reçu, il suffit de vérifier son empreinte grâce à un utilitaire.

Details	
Release	12.4.21
Size	25521384
BSD Checksum	-
Router Checksum	0x7aac
MD5	50018ababb6b3ae9ebc5c6a70123bdce
Date Published:	18-JUL-2008

L'empreinte MD5 est donnée dans ce tableau. Puis il faut effectuer un copier-coller de cette information dans l'outil de vérification dans lequel on charge également l'IOS à vérifier.



Nous observons ici que l'empreinte copiée à partir du site Internet correspond à celle de l'IOS téléchargé. Cependant, il est toujours possible de corrompre une image lors de son transfert. Fort heureusement, les équipements disposent d'une fonction qui vérifie l'empreinte de l'IOS au moment de son transfert. Cette fonction s'active avec la commande `file verify auto`. Une fois cette commande passée, les images seront vérifiées à chaque téléchargement dans l'équipement et en cas d'échec lors de la vérification l'image sera effacée. Il est à noter que cette commande effectuera aussi une vérification systématique de l'image en place dans l'équipement lors de sa réinitialisation.

b. Protection des mots de passe

La politique de sécurité impose une protection logique du routeur. Nous avons à plusieurs reprises dans les chapitres précédents créé des comptes d'utilisateurs distants auxquels nous avons systématiquement associé un mot de passe qui naturellement se retrouve dans la configuration. Il s'agit donc de protéger efficacement ce mot de passe au cas où la configuration viendrait à tomber entre de mauvaises mains. Cisco propose deux méthodes de chiffrement pour les mots de passe, nous disposons pour notre part d'un levier qui est la complexité du mot de passe. En la matière il convient de se référer à la partie de la politique de sécurité traitant de la génération des mots de passe et d'appliquer la complexité requise.

Il existe donc deux types de protection des mots de passe dans les configurations.

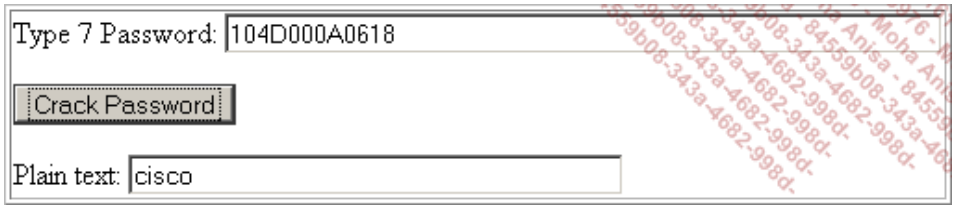
La première méthode applique un algorithme hélas réversible qu'il faut éviter autant que possible.

```
enable password 7 02050D480809
!
```

© ENI Editions - All rigths reserved - Moha Anisa

```
username vincent password 7 01100F175804
!
line vty 0 4
 password 7 104D000A0618
 login
```

Voici un exemple de ce chiffrement réversible utilisé pour protéger les accès Telnet. Il est identifiable grâce au chiffre 7 après le mot `password`.



De nombreux sites web permettent de décoder le chiffrement de type 7. Ici, quelle que soit la complexité du mot de passe il est récupérable. Notez qu'il est indispensable au préalable d'activer la commande `service password-encryption`.

La seconde méthode utilise une version de MD5 modifiée par Cisco qui n'est pas directement réversible.

```
R0(config)#enable secret cisco
!
R0(config)#username vincent secret cisco
```

En entrant les commandes ci-dessus, nous obtenons lors de la revue de la configuration ceci :

```
enable secret 5 $1$m3hk$LpKovptYw61uMDjauPeCt0
!
username vincent secret 5 $1$OCOM$75BPe3ttOA.dUPKsjxdd61
```

Ici, nous observons l'empreinte MD5 du mot de passe *enable* et celle du mot de passe d'un utilisateur.

Le chiffrement de type 7 qui protège le mot de passe d'accès aux lignes virtuelles devrait être systématiquement écarté au profit d'un protocole sécurisé tel que SSH. Ce dernier s'appuie sur une authentification pesonnalisée (éventuellement locale) et se configure comme suit.

```
R0(config)#aaa new-model
R0(config)#aaa authentication login default local
```

Cette configuration seule suffit à protéger avec un compte local les interfaces Telnet (vty), Console (con 0) et Auxiliaire.

Cisco met à disposition une commande qui permet de configurer un mot de passe à usage unique avec la commande `one-time` utilisée dans une séquence comme celle-ci : `username vincent one-time secret cisco`. Cette technique est applicable à une stratégie d'installation à distance d'un équipement disposant d'une configuration minimale. Un administrateur se connecte en SSH à l'équipement avec le mot de passe unique puis y télécharge une configuration plus complète comportant des éléments confidentiels avant de la sauvegarder dans la mémoire avec la commande `wr`. Le mot de passe unique est à ce moment-là définitivement perdu et remplacé par le compte définitif.

L'utilisation de compte locaux de préférence limitée à un compte afin d'exposer le moins possible l'équipement aux attaques qui tentent de s'en emparer. Il est habituellement considéré comme un compte de secours. En effet, il est recommandé d'accéder au routeur par le biais d'un compte hébergé sur une base externe à l'équipement comme celle d'un serveur de type RADIUS ce dernier interrogeant éventuellement à son tour une autre base de compte.

c. Protection des clés de chiffrement

Nous avons abordé le sujet de la protection des clés de chiffrement dans le chapitre traitant d'IPSec. Pour mémoire les commandes à utiliser sont : `key config-key password-encrypt` et `password encryption aes`.

Il ne faut pas limiter la protection des clés de chiffrement à la seule configuration. Les clés de chiffrement une fois générées sont idéalement conservées dans un lieu sûr et font l'objet d'une comptabilité soignée quant à leur attribution, à leur changement et à leur destruction. La gestion des clés sur un média électrique implique une protection de celui-ci par un chiffrement adéquat.

© ENI Editions - All rigths reserved - Moha Anisa

© ENI Editions - All rigths reserved - Moha Anisa

Conclusion

La protection des équipements, si elle est négligée, facilite considérablement les agissements des personnes mal intentionnées mais favorise aussi les erreurs de configuration ou de manipulation. Les conséquences de tels manquements peuvent être dramatiques et difficilement repérables en cas, par exemple, d'un mauvais réglage de l'heure.

Il en va de même pour l'environnement physique des équipements qui ne saurait souffrir d'aucune négligence car la préservation des performances et la durée de vie d'un équipement dépendent de facteurs sensibles comme la température ou l'hygrométrie.

Les journaux, en fonction de leur utilisation, sont à protéger durant leur transit sur le réseau et sur leur lieu de stockage afin qu'ils puissent le cas échéant servir de preuve lors d'une enquête consécutive à un accident, une panne ou un acte de vandalisme.

Enfin, il est fortement recommandé de faire suivre aux clés de chiffrement un cycle vie strict allant de leur génération à leur mise en service jusqu'à leur destruction.

© ENI Editions - All rigths reserved - Moha Anisa

Introduction

Pour certains, c'était un phénomène de mode mais pour d'autres c'était une nécessité. Éliminer à tout jamais des caves et des sous-sols les encombrantes armoires téléphoniques, les centraux et les autocommutateurs. La téléphonie classique, analogique puis numérique, était pour les entreprises un centre de coût sans cesse croissant avec l'embauche de nouveaux collaborateurs chacun nécessitant l'installation d'un poste téléphonique et la consommation d'un certain volume de communications. À cela s'ajoute le phénomène de mondialisation de l'économie qui a pour sa part grandement contribué à l'accroissement considérable des échanges téléphoniques nationaux et internationaux.

Jusqu'à une dizaine d'années, dans le domaine des télécommunications, la téléphonie véhiculait l'informatique et l'on trouvait dans les salles machines bon nombre de modems (modulateurs démodulateurs) raccordés à des lignes téléphoniques ouvertes en permanence. Ces liaisons extrêmement coûteuses permettaient de relier les gros systèmes informatiques entre eux et d'en assurer la maintenance à distance. Tout cela fonctionnait fort bien mais, de lignes louées analogiques en cartes d'extension en passant par le coût des appels longue distance, la facture télécommunication croissait chaque année un peu plus.

Avec l'avènement d'Internet et les progrès en matière de numérisation de la voix sont apparus au fil des années des logiciels permettant d'établir une communication vocale sur le réseau des réseaux avec des correspondants déjà connectés. Le pas vers la téléphonie sur IP fut rapidement franchi et les constructeurs comprirent qu'ils pourraient sans tarder proposer aux côtés de leurs produits phares des équipements qui permettraient de remplacer définitivement les centraux téléphoniques. À grand renfort de publicité et de communication les entreprises prirent conscience également qu'au-delà des premiers investissements, la téléphonie sur IP et les services associés diminueraient considérablement les coûts tout en accroissant la souplesse et la productivité.

À présent, les réseaux informatiques véhiculent le téléphone. Cette transition n'aura pas duré une décennie.

Nous allons dans ce chapitre énumérer les menaces qui planent sur les réseaux hébergeant des services de téléphonie sur IP et présenter les mesures de protection adéquates.

Le téléphone IP sur son poste de travail. C'est chose possible avec *Cisco IP communicator* un téléphone logiciel ressemblant comme deux gouttes d'eau aux modèles de la série 74XX.

© ENI Editions - All rigths reserved - Moha Anisa

Stratégie et sécurité

Le téléphone fait depuis plus d'un siècle partie de notre vie au point qu'il passe totalement inaperçu car il est un objet de consommation courante et le service qu'il fournit est particulièrement stable. Les réseaux téléphoniques sont les nerfs de notre civilisation moderne dont dépend notre mode vie au point qu'ils revêtent une dimension stratégique sans équivoque. C'est sans doute pour cette raison qui furent et restent encore dans une moindre mesure sous le contrôle des états qui peu à peu cèdent des licences d'exploitation à des compagnies privées. Le cœur des réseaux de télécommunication et toute son infrastructure sont ainsi protégés et surveillés avec la plus grande attention tant leur arrêt et l'interruption de service qui s'en suivrait auraient des conséquences désastreuses sur notre économie et notre vie courante. Il suffit pour cela de songer un instant à l'impossibilité de joindre un service de secours ou à l'incapacité de ces mêmes services à se coordonner en cas de catastrophe. Il en va de même dans le domaine économique. Pour toutes ces raisons, la sécurité des réseaux de télécommunication est fondamentale.

Nous allons examiner dans ce chapitre la sécurité des réseaux informatiques transportant les services de téléphonie sur IP plus connu sous le signe TOIP pour *Telephony Over IP*. Les services de TOIP supplantent les services classiques de téléphonie analogique ou numérique car ils s'intègrent parfaitement à l'infrastructure des entreprises dont ils partagent la capacité avec les autres services comme la messagerie. Le succès que connaissent actuellement les services de téléphonie sur IP sont en partie du à cette étroite imbrication qui diminue considérablement sur le long terme les coûts d'exploitation de la téléphonie classique. Ainsi, il n'est plus nécessaire de maintenir un câblage spécifique en parallèle de celui destiné au réseau informatique. De plus, les services de TOIP sont hébergés sur des serveurs au même titre que toutes les autres applications.

C'est hélas en partie à cause de ces avantages que les réseaux TOIP entrent dans la problématique générale de la sécurité informatique. En fait, ils héritent tout naturellement des mêmes menaces et des mêmes faiblesses. Examinons-les.

1. Menaces et faiblesses

Au chapitre des menaces et faiblesses planant sur les réseaux de TOIP nous trouvons les attaques par déni de service qui prennent ici une dimension mesurable par tous les utilisateurs d'un réseau téléphonique. Nous nous sommes en effet habitués année après année à une excellente disponibilité du réseau téléphonique domestique et à une amélioration constante de la qualité de la voix de nos correspondants. Rares sont de nos jours les problèmes de distorsion ou de diaphonie et notre interlocuteur nous paraît naturellement proche. Toutefois, les réseaux de téléphonie sur IP souffrent d'autres imperfections comme l'écho qui dépend étroitement du temps d'acheminement des paquets sur le réseau et le hachage des conversations dès que la bande passante vient à manquer. Les attaques par déni ou dégradation de service disposent donc d'un terrain favorable du fait même de la technologie utilisée. Les attaques portent principalement sur les équipements du réseau ou sur les serveurs hébergeant les services de téléphonie sur IP, ces derniers ayant remplacé les traditionnels centraux téléphoniques. Les attaques ne manquent pas et consistent à rendre un poste indisponible en le faisant sonner sans cesse ou en diffusant un message en boucle après avoir décroché le combiné. Quant au cœur du système toutes les techniques visant à mettre hors service un serveur sont théoriquement utilisables.

Les écoutes téléphoniques nourrissent tous les fantasmes depuis l'apparition du téléphone et donnent toujours lieu à d'importants scandales politico-médiatiques. À ce titre elles attirent toujours l'attention des curieux en tout genre. Les écoutes s'opèrent au sein de deux périmètres bien distincts, ce sont le voisinage direct de l'appareil à piéger ou le réseau de l'opérateur. C'est sur ce dernier qu'opèrent les services gouvernementaux qui seuls ont le droit sous couvert de la justice de pratiquer les écoutes. Le voisinage direct du poste téléphonique s'étend du poste lui-même à l'entrée sur le réseau de l'opérateur téléphonique. Pour mémoire, au voisinage du poste, les écoutes des réseaux analogiques ne nécessitaient que très peu de matériel, un simple fer à souder et des pinces crocodiles étaient amplement suffisants. Puis, la téléphonie avant de basculer dans l'univers IP que nous allons décrire est passée par une étape intermédiaire pendant laquelle la voix, déjà numérisée, cheminait sur un protocole informatique nommé RNIS. Les écoutes sur le réseau au voisinage des appareils requéraient la mise en œuvre d'appareil dérivés des analyseurs de ce protocole. Les écoutes n'étaient dès lors plus à la portée du premier venu car le matériel était assez coûteux. Avec l'avènement de la TOIP, nous pouvons dire qu'en matière de sécurité s'opère un certain retour en arrière car cette technologie, si rien n'est fait pour la protéger, redevient sujette aux écoutes avec des moyens relativement simples et surtout très largement diffusés. Fort heureusement, pour pallier cet état de fait, des mesures de protection sont disponibles.

L'un des multiples cauchemars d'un responsable de la sécurité veillant sur un réseau fournissant des services de TOIP est la fraude. Ce terme désigne au sens large les appels sortant du périmètre de l'entreprise vers des services payants ou des contrées lointaines. La facture téléphonique augmente considérablement et les agissements des fraudeurs doivent être entravés le plus rapidement possible. Les méthodes utilisées descendent en ligne directe de celles utilisées du temps de la téléphonie analogique et consistent à manipuler des préfixes ou à jouer des mécanismes de redirection d'appel.

2. Mesures de protection

Les mesures de protection ne manquent heureusement pas pour entraver les attaques que nous venons brièvement

© ENI Editions - All rigths reserved - Moha Anisa

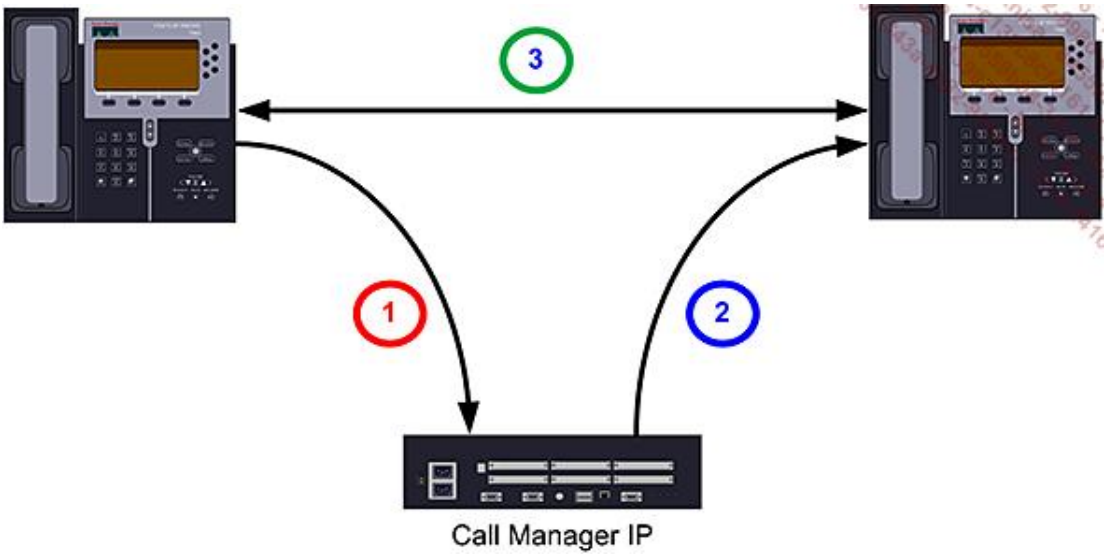
d’évoquer. Tout comme la TOIP repose sur les réseaux de données IP en héritant des problèmes de sécurité, elle hérite aussi des méthodes de défense qui vont s’articuler autour du réseau et des équipements que sont les téléphones et les serveurs de voix sur IP.

Au niveau physique, une dose de protection s’avèrera nécessaire pour ne pas nuire à l’intégrité du téléphone IP et encore moins à celle des serveurs. La couche 2 du modèle OSI sert, à l’instar de ce que nous avons déjà examiné, à lancer des attaques d’interception du trafic dont le but ultime n’échappera à personne. Les couches session et réseau sont extrêmement sollicitées par la téléphonie sur IP qui est fortement consommatrice de ports attribués dynamiquement et qu’il conviendra de limiter et de filtrer avec le plus grand soin. La couche application quant à elle n’est pas en reste car les serveurs ainsi que les téléphones sont les victimes d’attaques diverses tant au niveau des protocoles de voix sur IP qu’au niveau des diverses interfaces d’administration qu’il convient de protéger avec soin par le biais de protocoles HTTPS ou SSH tout en veillant à déconnecter les sessions ouvertes après un temps d’inactivité raisonnable.

© ENI Editions - All rigths reserved - Moha Anisa

La vision de Cisco

Cisco propose depuis le milieu des années 90 un service de téléphonie sur IP intégré connu sous l'appellation de Call Manager mais dont le nom commercial actuel est CUCM pour *Cisco Unified Communication Manager*. Ce véritable central téléphonique IP (on parle d'IPBX) outre ses capacités à gérer des milliers d'appels offre toute une gamme de services annexes comme la mobilité, la présence ou encore les conférences. Cisco fournit avec son système un protocole propriétaire de téléphonie sur IP nommé SCCP (ou *Skinny*), il est réputé pour sa légèreté comparativement au protocole H323. SCCP est actif entre le téléphone IP et le Call Manager pour l'établissement d'un appel. Examinons très schématiquement le déroulement d'une communication.



Nous observons sur ce schéma simple l'établissement d'une communication entre deux postes téléphoniques IP. La méthode descend en ligne directe de celle mise en œuvre par la téléphonie analogique.

1 - L'appelant décroche son combiné et compose le numéro de son correspondant. Dès le décroché du combiné, le serveur TOIP détecte une activité et attend la numérotation avant de l'interpréter.

2 - Le serveur de TOIP cherche la correspondance entre le numéro composé par l'appelant et l'adresse IP du correspondant et lorsqu'il la trouve fait sonner la ligne. En retour, il annonce cet état à l'appelant qui reçoit la tonalité de sonnerie.

3 - Le correspondant décroche son combiné. Le serveur TOIP informe alors les deux correspondants sur leurs adresses IP respectives et les ports à utiliser afin d'entamer la communication. À l'issue, le serveur TOIP se retire et laisse les deux correspondants échanger librement des paquets contenant de la voix numérisée.

Les étapes numérotées 1 et 2 sont désignées en termes téléphoniques comme étant le protocole de signalisation ou par extension de langage : la signalisation. L'étape numéro 3 constitue la conversation téléphonique proprement dite et fait appel à d'autres protocoles.

Nous pouvons déjà à partir de ce simple schéma aborder les cas dans lesquels la sécurité serait menacée. Toutefois, les architectures TOIP ne se limitent pas à ce modèle car les architectures les plus complexes prévoient des points de sorties vers les réseaux public via des passerelles spécialisées. Certains réseaux de TOIP mettent aussi en œuvre des équipements destinés à la conversion entre les protocoles TOIP, mais nous examinerons pour plus de clarté des cas de figure relevant de l'exemple décrit dans ce schéma.

© ENI Editions - All rigths reserved - Moha Anisa

Exigences de sécurité et solutions

Les versions de CUCM évoluent sans cesse, aussi nous avons décidé de ne pas encombrer le lecteur de multiples écrans de configuration et avons choisi de décrire les menus conduisant à la configuration souhaitée tels qu'ils existent dans la version 6.0.1.

Nous pouvons déjà à partir du simple schéma décrivant une communication aborder les cas dans lesquels la sécurité serait menacée. Toutefois, les architectures TOIP ne se limitent pas à ce modèle car les architectures les plus complexes prévoient des points de sorties vers les réseaux public via des passerelles spécialisées. Certains réseaux de TOIP mettent aussi en œuvre des équipements destinés à la conversion entre les protocoles TOIP. Pour plus de clarté, nous n'examinerons que des cas de figure relevant de l'exemple décrit dans ce schéma.

L'objectif de ce chapitre est de décrire les principales menaces qui pèsent sur un réseau TOIP et de les contrer grâce aux mesures de protection déjà implémentées sur un réseau IP et celles propres aux services de téléphonie. La politique de sécurité de l'entreprise hérite d'un nouveau chapitre avec l'avènement des services de TOIP, chapitre dont nous verrons qu'il est étroitement lié à celui sur la sécurité aux niveaux deux et trois du modèle OSI.

Les écrans de ce chapitre proviennent de la version 6 de Cisco *Unified Communication Manager*.

1. Exigences liées à la sécurité réseau

Exigences de sécurité physiques et réseau appliquées à la TOIP	
Protection des services de TOIP.	Protection physique des locaux.
Protéger physiquement et logiquement les équipements d'extrémité.	Surveillance des bureaux sensibles. Désactivation de l'interface Web
Assurer la séparation du trafic voix et données.	Mise en place de VLAN dédiés à la voix et filtrage entre les VLAN.
Interdire les attaques de type man in the middle.	Dispositifs de surveillance au niveau 2. Non écoute des messages gratuitous ARP.

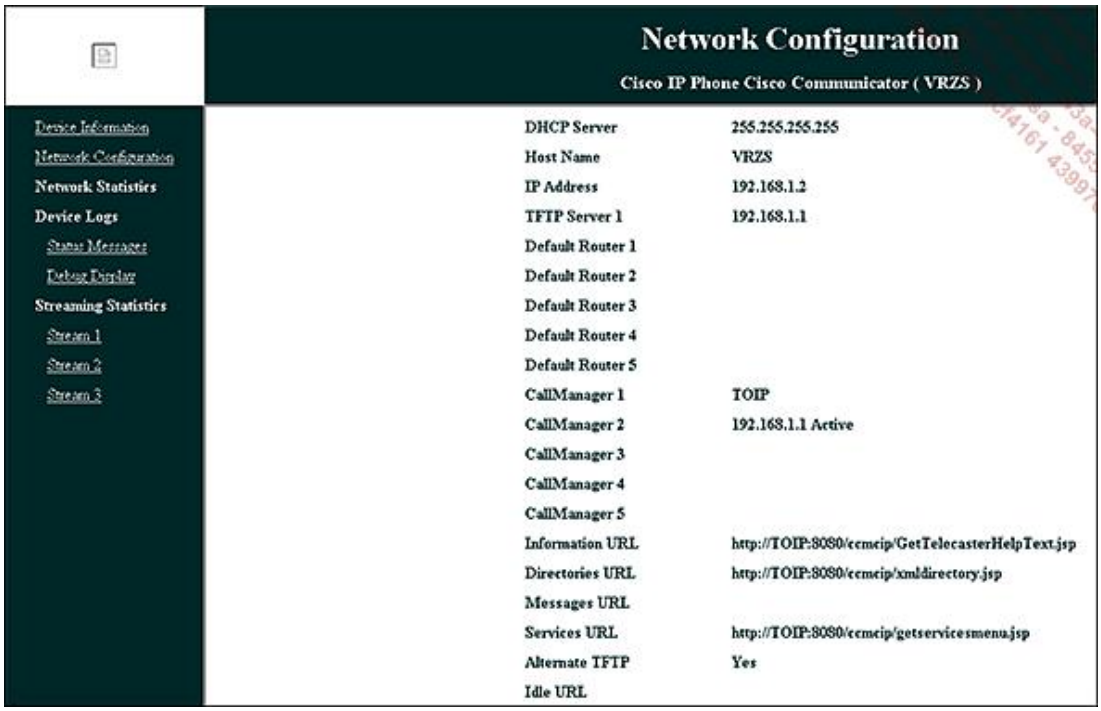
Les services de téléphonie sur IP sont, nous l'avons souligné, stratégiques et ne sauraient souffrir d'aucune panne. Ceci est en partie dû à l'excellente fiabilité à laquelle nous sommes habitués de la part des réseaux téléphoniques précédents.

Maintenir un tel niveau de disponibilité nécessite une haute protection physique des services. Toutes les règles évoquées précédemment sont à disposition afin d'atteindre cet objectif.

Les appareils d'extrémité comme les téléphones IP et les stations de téléconférence doivent être l'objet d'une attention toute particulière car leur intégrité physique garantit directement le niveau de confidentialité de toute la chaîne de communication. Avant d'aborder l'impérieuse nécessité de chiffrer les communications et la signalisation, il est indispensable de préciser que les attaques les plus audacieuses portent directement sur les équipements avant même que tout chiffrement intervienne. Il s'agit alors de piéger les micros ou écouteurs c'est-à-dire les composants chargés de capter la voix humaine ou de la restituer. Ainsi, un micro émetteur habillement dissimulé dans un combiné contourne toutes les mesures de protection prises en aval comme le chiffrement car il intervient avant la numérisation du signal et son chiffrement.

Certains postes de par leur position dans des locaux sensibles comme les salles de conférence doivent faire l'objet d'une attention soutenue par le biais par exemple de caméras de vidéo surveillance. Les équipements d'extrémités disposent parfois de microphones d'ambiance destinés à capter la voix lorsque le combine est raccroché ce qui permet de poursuivre une conversation les mains libres. Ces microphones sont généralement activables par le logiciel du téléphone et son interface d'administration. En cas de défaillance logicielle ou de négligence quant à la protection des accès à cette interface, les conversations pourraient transiter via ce microphone discrètement activé. Sa désactivation s'impose donc. De même, la plupart des téléphones IP disposent d'une interface d'administration Web qui peut enfreindre la politique de sécurité et se voir affectée de bugs logiciels.

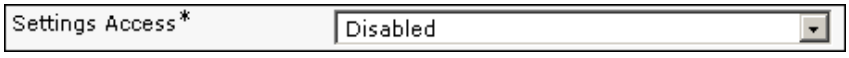
© ENI Editions - All rigths reserved - Moha Anisa



Voici ce que l'on obtient en se connectant en http à l'adresse IP du téléphone après s'être bien entendu connecté au VLAN voix. Cette page affiche quelques informations qui indiquent entre autres ses URL sur le CUCM qui permettent de se connecter en tant qu'utilisateur ou de lancer une attaque visant à trouver un couple d'authentification valide.

Nonobstant cette mesure, le téléphone présente à l'utilisateur par le biais des menus des informations sensibles de sécurité.

Ici, l'utilisateur visualise les options de sécurité de son téléphone et avec la combinaison de touches **# a la possibilité d'opérer quelques modifications. Tout comme pour le serveur HTTP embarqué, la présentation de la configuration à l'utilisateur est une option qu'il est préférable de désactiver.



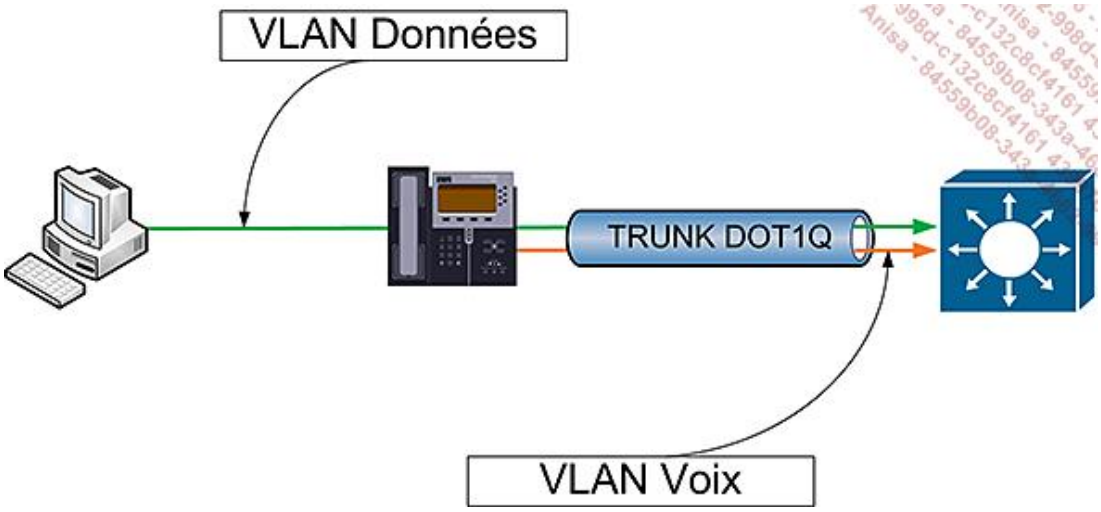
Les données issues des postes de travail et celles provenant des appareils de téléphonie sur IP doivent-elles emprunter le même chemin ? Les règles de sécurité que nous avons décrites recommandent une ségrégation du réseau en zones fonctionnelles. Il en va de même pour les données si elles sont issues d'origines qu'il convient d'isoler les unes des autres pour des raisons de confidentialité. Ceci est laissé à la discrétion de la politique de sécurité. En matière de téléphonie sur IP une séparation entre la voix et les données est recommandée afin entre autre de limiter l'impact d'une perturbation sur le réseau réservé aux données. Cette exigence de séparation repose quasi essentiellement sur les VLAN. Dans la pratique, deux approches sont envisageables :

- La première consiste pour un même utilisateur de dissocier la connexion du téléphone IP au réseau de celle de

© ENI Editions - All rigths reserved - Moha Anisa

l'ordinateur, chacun occupant un port sur l'équipement de raccordement.

- La seconde consiste à connecter l'ordinateur sur le téléphone ce dernier étant connecté via un *trunk* 802.1Q à l'équipement de raccordement. Cette dernière solution est la plus couramment employée car elle économise un port.



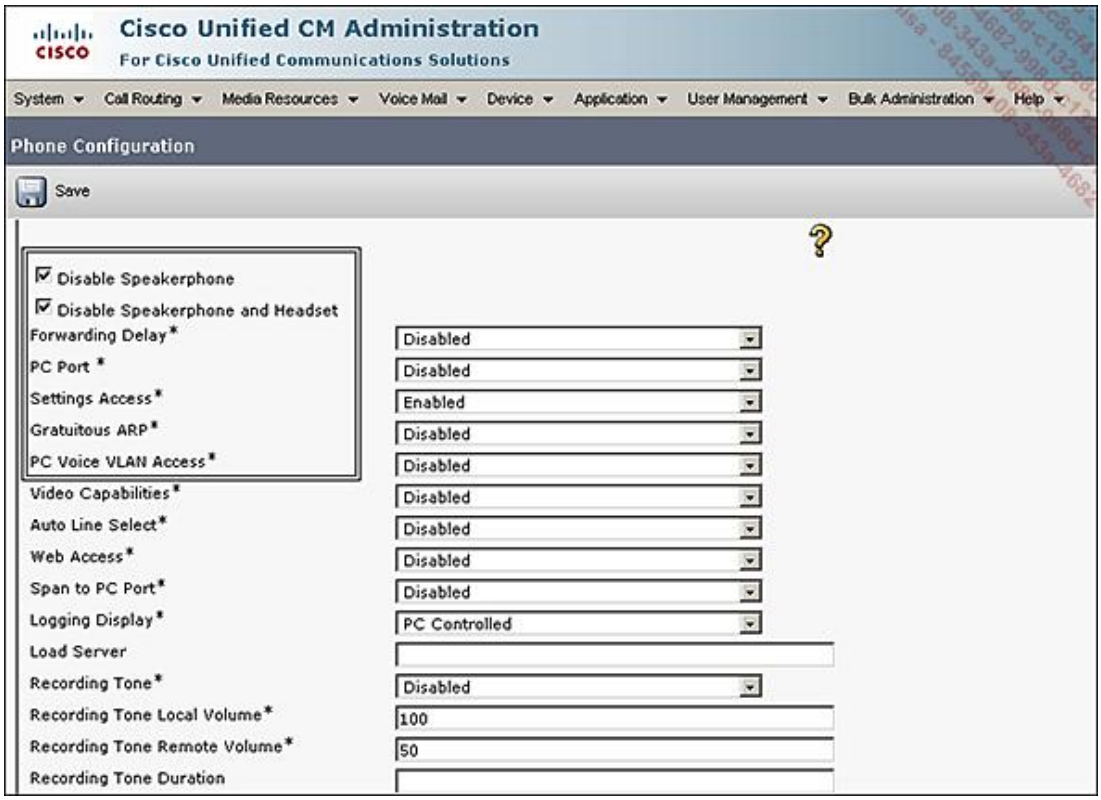
Ici, le téléphone joue le rôle d'un commutateur Ethernet en acceptant d'un côté un *trunk* composé de deux VLAN et de l'autre un ordinateur individuel. Un VLAN données accueille l'ordinateur et un VLAN voix reçoit les paquets émis par le téléphone IP.

Si cette configuration est déployée par défaut, le port réservé au PC sera partout disponible y compris sur les postes téléphoniques qui ne sont pas destinés à en recevoir un. Ceci entrave éventuellement la politique de sécurité en offrant une porte d'entrée au réseau sur un lieu public, il est alors indispensable d'avoir la possibilité de désactiver ce port.

Nous avons déjà abordé les problèmes posés par les attaques de type *man in the middle* au cours desquelles un tiers intercepte le trafic entre deux correspondants en trompant les systèmes d'exploitation au niveau de la couche 2 du modèle OSI. Cette attaque transposée dans le monde de la téléphonie sur IP signifie que les conversations seront écoutées à l'insu des correspondants légitimes. Les attaques sont également basées sur le protocole ARP et consistent à empoisonner le cache ARP d'un téléphone (*ARP poisoning*). L'arsenal qu'il convient d'employer est identique à celui décrit dans le chapitre sur la protection au niveau 2. En complément notons que la configuration d'un poste IP permet de désactiver tout ce qui n'est pas strictement nécessaire au fonctionnement de l'appareil comme l'acceptation des messages *gratuitous ARP*.

Le téléphone IP lors de son initialisation fait appel aux services d'un serveur DHCP pour obtenir son adresse IP. Les protections étudiées au chapitre La sécurité des couches physiques et liaison de données sont aussi à appliquer impérativement.

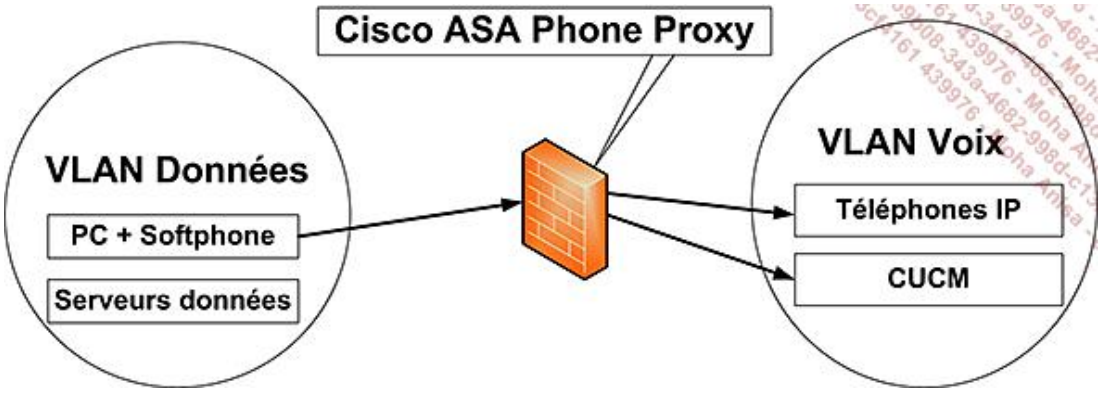
© ENI Editions - All rigths reserved - Moha Anisa



Voici une illustration des options dont nous venons de parler. L'accès au VLAN voix par le téléphone s'effectue lors de la première prise de contact grâce au protocole CDP dont nous savons qu'il est vulnérable à de multiples attaques d'où l'importance de veiller à l'isolation du PC par rapport au VLAN voix qui une fois découvert ouvre la porte potentiellement à bien des débordements. Ces options sont visibles dans l'onglet **Device**, puis dans l'onglet **Phone**. Il faut ensuite rechercher les propriétés d'un numéro ou créer un téléphone.

Si la séparation entre voix et données est effective grâce à l'emploi des VLAN, un nouveau problème se pose s'il est décidé de déployer des téléphones logiciels sur le réseau réservé aux données. Il s'agit de garantir en toute sécurité le passage du trafic provenant des téléphones logiciels vers le VLAN dédié à la voix. De plus, il est conseillé de ne pas laisser se connecter via le réseau de données un téléphone logiciel sans qu'il soit authentifié.

La solution proposée par Cisco est de forcer le passage de ce trafic par un firewall ASA qui se charge d'authentifier le téléphone logiciel avant de transmettre la signalisation vers le CUCM. Cette technique requiert la configuration de certificats sur le firewall qui, groupés dans un fichier CTL, sont proposés au téléphone ainsi qu'une obligation à s'authentifier.



2. Confidentialité et authentification

Le mythique téléphone rouge est à la portée de tous. Il est tout à fait possible de passer à son collègue de bureau un appel téléphonique chiffré, tout ceci n'est plus l'apanage des grandes puissances nucléaires et la technologie est tout aussi puissante que celle utilisée durant la tristement célèbre guerre froide.

Après avoir procédé à la configuration de la sécurité physique et réseau, il faut à présent examiner les mesures qui renforcent la confidentialité des échanges téléphoniques. En prenant pour référence le schéma montrant l'établissement d'une communication, des grandes phases principales se détachent et à chacune d'elles correspond

© ENI Editions - All rigths reserved - Moha Anisa

des mesures de sécurité. Posons les exigences en matière de confidentialité et d'authentification.

Exigences de confidentialité et d'authentification appliquées à la TOIP	
Assurer la sécurité de la signalisation.	Utilisation de TLS
Authentifier l'équipement d'extrémité.	Utilisation de TLS
Assurer la confidentialité et l'intégrité de la communication.	Utilisation de SRTP
Chiffrer les fichiers de configuration.	Dispositif de chiffrement des fichiers de configuration

Cisco recommande tout d'abord l'activation d'IPSEC en cas d'utilisation d'un groupement de serveurs redondants car il n'est pas prévu nativement de protection entre les serveurs. Concernant les communications et la signalisation, Cisco base sa solution sur la mise en œuvre d'une infrastructure de clés publiques (PKI) et le panel habituel des protocoles de sécurité dont TLS. Le chiffrement de la voix utilise quant à lui le protocole SRTP (*Secure Real Time Protocol*).

a. Protection de la signalisation

La signalisation est l'épine dorsale de tout système téléphonique car elle transporte entre autres la numérotation composée sur le cadran de l'appareil. D'une manière générale, une fois le combiné décroché, la signalisation entre en jeu pour d'une part informer l'utilisateur sur le succès de ses requêtes (diverses tonalités) et d'autre part pour informer le central téléphonique du numéro avec lequel il devra établir une liaison. Les protocoles de signalisation utilisés pour la téléphonie sur IP sont SIP, H 323 et SCCP qui est propriété de Cisco bien que quelques implémentations existent chez d'autres marques (IPBlue, Asterisk). La protection de la signalisation est un pré-requis pour l'échange sécurisé de média entre le CUCM et les équipements. La signalisation est donc un flux stratégique qu'il convient de protéger car toute attaque contre elle met en péril l'infrastructure téléphonique par une désorganisation en temps réel. Cela se manifeste entre autre par un taux élevé d'appel qui n'aboutissent pas correctement ou pas du tout.

La signalisation entre les téléphones et le CUCM est protégée par le protocole TLS (*Transport Layer Security*) qui a succédé à SSL (*Secure Socket Layer*). Dans le cas d'un réseau téléphonique entièrement chiffré (excluant pour l'instant les téléphones logiciels) aucune analyse du protocole n'est envisageable. Il est envisageable avec le firewall ASA, qui possède une fonction de proxy TLS et s'intercale entre un téléphone IP et le CUCM, de déchiffrer la signalisation venant du téléphone, d'en analyser les propriétés et de la chiffrer de nouveau avant de la diriger vers le CUCM. Cette technique nécessite la production de certificats et leur installation sur le firewall afin qu'il puisse s'interposer entre les téléphones et le CUCM.

b. Protection de la voix

Afin de combattre efficacement les écoutes téléphoniques, le chiffrement se pose comme une solution de choix. Le protocole mis à contribution se nomme SRTP (*Secure Real Time Protocol*) et se base sur deux protocoles bien connus qui sont AES (pour le chiffrement) et SHA (pour le contrôle d'intégrité). Un pré-requis à l'utilisation de SRTP est la protection de la signalisation car elle transporte les clés de chiffrement de la voix. SRTP est défini par la RFC 3711.

c. Protection des médias (images et configurations)

L'authentification des images ou des configurations permet d'éviter qu'un équipement reçoive un logiciel corrompu ou piégé par un tiers. Le processus de vérification des images est indépendant du CUCM. Les produits logiciels destinés aux équipements de téléphonie sont signés électroniquement lors de leur production par Cisco.

Il est enfin recommandé d'authentifier et de chiffrer les fichiers de configuration reçus par le téléphone et provenant du serveur TFTP, ces fichiers comportent en effet quelques informations sensibles. L'activation de cette fonctionnalité est facilitée si le téléphone est détenteur d'un certificat dans le cas contraire un code est entré au clavier avant le téléchargement du fichier de configuration.

Nous venons d'aborder des fonctionnalités particulièrement utiles pour la protection des divers échanges entre les composants de l'infrastructure de téléphonie IP. Toutefois, rien de tout ceci ne serait envisageable sans une méthode d'authentification entre les éléments qui composent cette infrastructure. Le CUCM embarque à cet effet une PKI dont tâche est la production de certificats X509 destinés aux divers composants de service du CUCM et aux téléphones.

d. L'infrastructure à clé publique du CUCM

© ENI Editions - All rigths reserved - Moha Anisa

Avant toute chose, il est important de souligner les difficultés qui accompagnent toujours le déploiement d'une architecture de clés publiques ou PKI en anglais. Le travail à fournir s'articule autour de problématiques techniques et organisationnelles. Ainsi, la phase d'étude ne saurait être négligée au bénéfice de la phase technique et vice-versa.

Dans le cadre du CUCM se trouvent au moins trois autorités de certification (CA) qui sont les CUCM, les serveurs TFTP et le CAPF (*Certificate Authority Proxy Function*). Nous sommes également en présence de trois types de certificats qui se différencient en fonction de l'autorité par laquelle ils ont été signés. Ce sont :

- les certificats auto-signés par les serveurs centraux pour leurs propres besoins (accès administratifs en HTTPS) ;
- les certificats signés par les processus de fabrication directement chez Cisco sont appelés MIC (*Manufacturing Installed Certificate*) ;
- les certificats signés par le CAPF ou par une CA externe sont appelés LSC (*Locally Significant Certificates*).

Les téléphones IP en fonction de leur modèle reçoivent un certificat MIC lors de leur fabrication ou s'il n'en sont pas munis devront recevoir un certificat LSC en vue d'utiliser les fonctions de chiffrement.

Des certificats émis par des autorités de certification différentes ne pourront s'authentifier mutuellement qu'à condition que leurs autorités respectives dépendent d'une autorité supérieure commune. C'est le principe de la chaîne de certification. Cisco pour regrouper les multiples autorités de certification qui composent l'architecture CUCM propose un logiciel nommé CTL Client (*Certificate trust List Client*) dont la fonction est d'interagir avec une clé de sécurité USB (*eToken*) qui signe la liste des certificats des autorités de certification. Cette liste (signée) est chargée dans chaque téléphone lors de son démarrage. Lors d'un processus d'authentification préalable à une procédure de chiffrement, le téléphone examine le certificat qu'il reçoit de son partenaire et le confronte à la liste CTL qu'il possède.

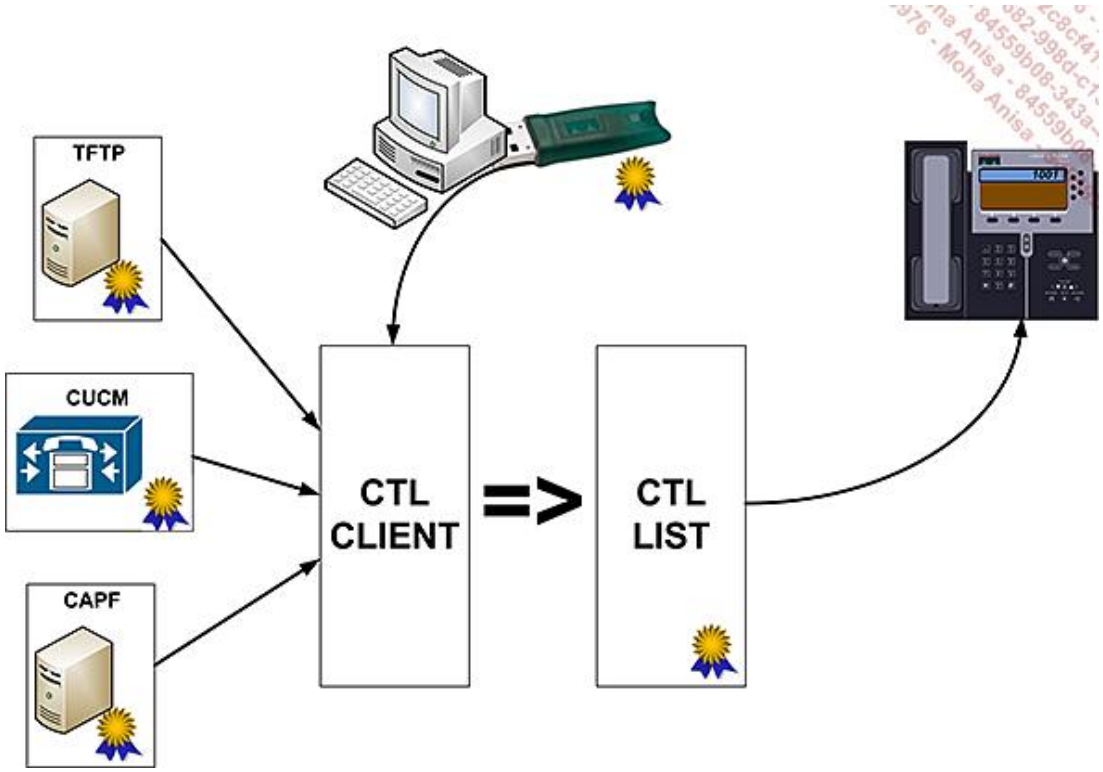
Le logiciel CTL Client est téléchargé sur une station de travail à partir d'une page de l'interface d'administration du CUCM réservée aux *plug-ins* et aux *API* et nécessite une clé USB de sécurité du type *eToken* sur laquelle seront déposés les clés privées et les certificats des autorités de certification.

eToken Cisco

Cette clé USB est un élément de sécurité qui porte l'appellation d'*eToken* renferme une paire de clé (publique signée et privée) générée par Cisco.

Le principe de la CTL est comparable à celui de la liste blanche qui définit les CA autorisées à valider un certificat au contraire d'une CRL (*Certificate Revocation List*) qui est une liste de certificats interdits.

© ENI Editions - All rigths reserved - Moha Anisa



Lors du premier chargement d'une CTL, un appareil qui n'en possède pas acceptera sans autre forme de procès une CTL quelle que soit son origine. Le réseau sur lequel s'effectue cette première installation doit être irréprochable.

Une fois la PKI activée (l'opération n'est pas triviale) les téléphones sont configurés pour utiliser le protocole de signalisation chiffré préalablement défini dans un profil puis s'enrôlent auprès du CUCM.

La cryptographie correctement configurée au niveau des équipements et du protocole de signalisation, les téléphones ayant la capacité d'entamer une conversation protégée entre eux le font naturellement en procédant à une vérification mutuelle de leurs certificats. Des modes dégradés sont toutefois envisageables pour les téléphones ne possédant pas toutes les fonctions de sécurité. C'est le cas des téléphones logiciel (*Softphones*) du type *Cisco IP communicator* qui ont seulement la capacité de protéger la signalisation.

3. Lutte contre la fraude

La lutte contre la fraude est une priorité pour les entreprises afin de ne pas s'exposer à des comportements dangereux et irresponsables pouvant engendrer des facturations très lourdes. Le phénomène remonte aux origines même de la téléphonie. Les entreprises offrent à leurs collaborateurs quelques facilités qui si elles ne font l'objet d'aucune surveillance sont un facteur aggravant du phénomène de fraude. L'information concernant la découverte d'une martingale s'échange entre initiés et le montant des factures qui connait dans les premiers temps une croissance modérée « explose » quelques mois plus tard. Il est à noter que la fraude ne revêt pas systématiquement un caractère technique par le biais de savantes manipulations, mais consiste parfois en une utilisation déraisonnable des moyens octroyés au collaborateur. Citons à titre d'exemple les postes bénéficiant d'un accès à l'international utilisés par des utilisateurs malveillants dès le départ en fin de journée du titulaire de la ligne. Une utilisation abusive est aussi considérée comme une fraude à part entière.

La fraude qui met à profit une utilisation indirecte de la ligne s'appuie donc très fréquemment sur les facilités offertes par le central téléphonique IP. Les services de redirection d'appel s'il ne sont pas sécurisés permettent de rediriger un appel entrant (provenant de l'extérieur de l'entreprise) vers un service surtaxé ou un pays exotique. De même un appel interne peut se voir redirigé vers l'extérieur. Ces méthodes nécessitent un complice parmi les collaborateurs à moins que le bénéficiaire n'opère seul. Les services de boîte vocale permettent aussi sous certaines conditions de bénéficier d'une fonctionnalité de redirection d'appel.

Nous ne présentons pas ici comme à l'accoutumée un tableau d'exigences car la lutte contre la fraude est une exigence unique dont il est possible de se prémunir avec les configurations que nous allons examiner.

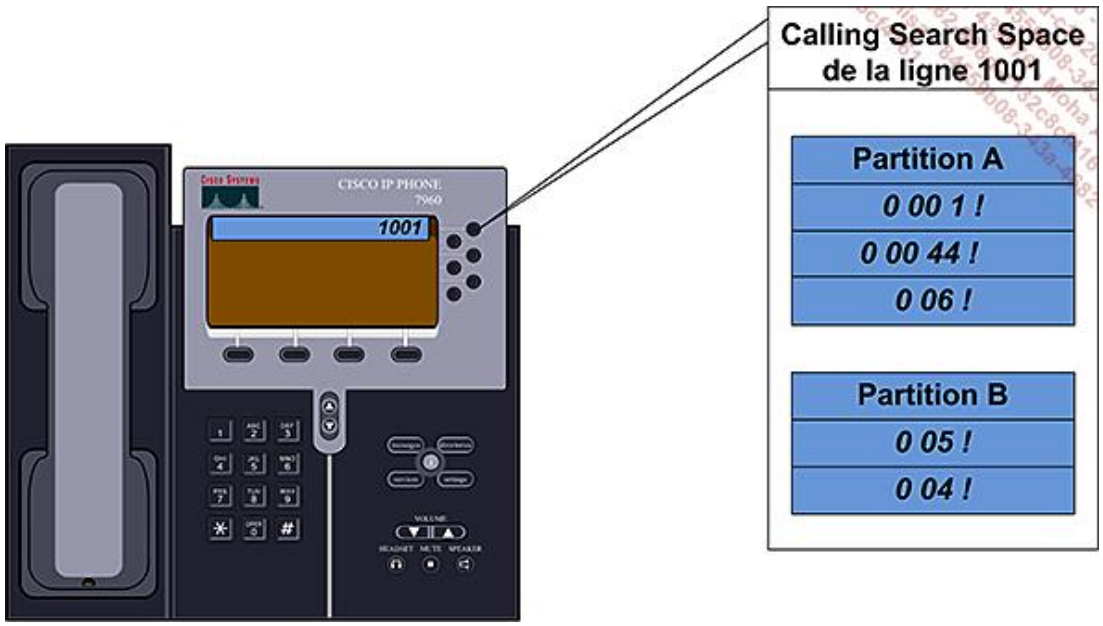
a. Techniques anti-fraude

Les techniques permettant de restreindre les possibilités de contrôler la redirection ou les appels sont basées sur l'analyse du numéro composé. Nous savons par exemple qu'en France, un appel international débute toujours par la séquence (ou préfixe) "00", de plus, à l'intérieur de l'entreprise, il faut traditionnellement ajouter un "0" pour indiquer un appel vers l'extérieur. La séquence de numérotation débute donc par "000". Le logiciel d'exploitation du

© ENI Editions - All rigths reserved - Moha Anisa

central téléphonique IP est en conséquence configuré pour reconnaitre toutes les séquences (en anglais patterns) qui correspondent aux destinations internes, nationales, internationales et à divers services. Schématiquement, pour filtrer les appels ou les redirections la marche à suivre est la suivante :

- définition des groupes de préfixes de numérotation (0 00 33 ; 0 00 44 ;…) ;
- créations de groupes d'utilisateurs en fonction de leurs privilèges ;
- regroupement des groupes d'utilisateurs et des groupes de préfixes afin de déterminer les destinations permises aux membres des groupes.



Les trois points que nous venons de décrire sont représentés sur le schéma ci-dessus et se traduisent par la terminologie Cisco suivante :

- dans le menu **call routing**, le sous-menu **translation pattern** permet de créer les séquences qui sont comparées avec le numéro composé. Des caractères spéciaux sont prévus à la manière des *scripts shell* (Unix/Linux) pour désigner des séquences ou des suites de chiffres. Par exemple la séquence 000*1!* désigne tous les numéros de téléphone commençant par les chiffres 000*1* suivi de n'importe quel autre chiffre.
- une **partition** est un ensemble de *pattern* qui groupés sont applicables à une ligne téléphonique IP. Toutefois, les numéros ne correspondant à aucun *pattern* ne seront pas joignables sans l'aide des espaces de recherches d'appel les *calling call space*.
- les **calling call space** regroupent des partitions selon un certain classement. Ils sont appliqués à un équipement téléphonique IP comme un téléphone ou à une ligne comme indiqué sur le schéma.

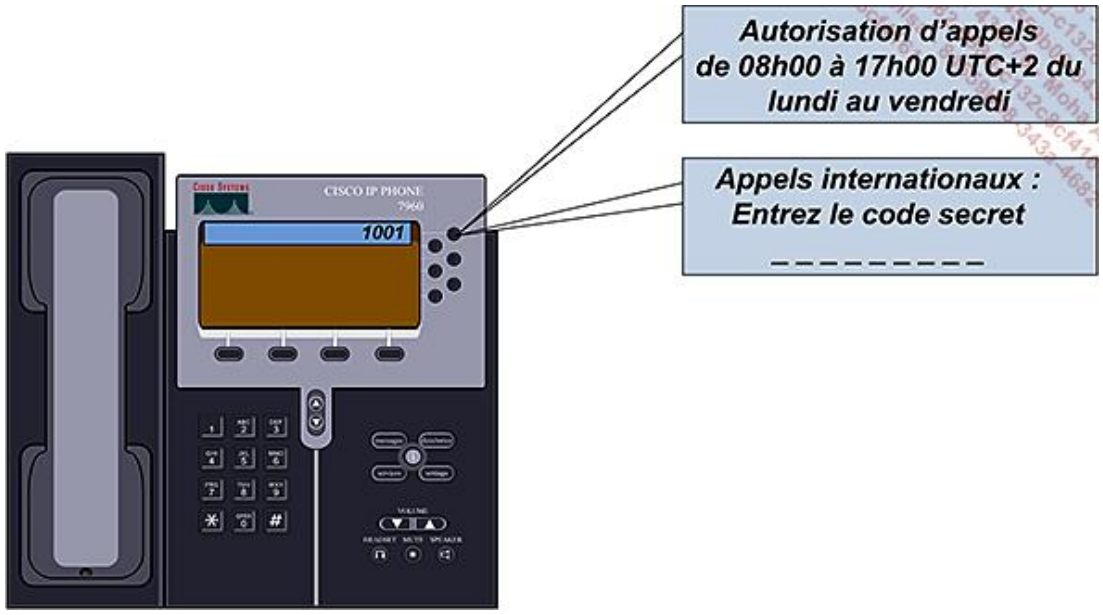
Deux termes importants sont utilisés ici et méritent un éclaircissement car ils couvrent la notion de poste téléphonique et de ligne téléphonique. Au début de ce chapitre figure l'image d'un téléphone logiciel IP. Sur la gauche de l'image se trouvent huit boutons ronds matérialisant huit lignes téléphoniques potentielles dont seule la première est configurée pour un utilisateur. Par déduction, un poste téléphonique est un objet (logiciel ou physique) qui peut recevoir une ou plusieurs lignes téléphoniques.

	Direction	**Encadrement**	**Employés**
Appels internationaux Europe	OK	OK	X
Appels internationaux Amérique du nord	OK	OK	X
Appels internationaux autres destinations	OK	X	X

© ENI Editions - All rigths reserved - Moha Anisa

Appels nationaux	OK	OK	X
Appels vers les mobiles	OK	OK	X
Appels régionaux	OK	OK	OK
Numéros d'urgence	OK	OK	OK

Voici un tableau relatif aux appels ou aux redirections en fonction d'une position hiérarchique dans l'entreprise. À chaque case OK correspond la possibilité d'établir ou de rediriger un appel vers les préfixes appartenant aux familles de la colonne de gauche. Le CUCM offre deux autres techniques complémentaires à celles que nous venons d'étudier :



- La limitation des appels en fonction de l'heure et du jour de la semaine. Cette méthode nécessite la définition d'un *time period* à reporter dans un *time schedule* à déclarer dans une *partition*. Cette dernière est à déclarer dans un *calling search space* lui-même appliqué à un équipement ou à une ligne.

- L'obligation faite à un utilisateur d'entrer un code secret préalablement à un appel et ce, en fonction du préfixe et d'une priorité entre le niveau d'autorisation de ce préfixe et celui de la route téléphonique qu'il doit emprunter.

Ces descriptions peuvent paraître relativement abstraites il est donc fortement recommandé de se reporter au manuel du CUCM pour de plus amples explications relatives à la configuration.

Une route téléphonique est un chemin vers l'extérieur du domaine, en général vers le réseau téléphonique public. Cette notion est proche de celle d'une route IP qui serait extérieure au réseau local.

© ENI Editions - All rigths reserved - Moha Anisa

Conclusion

Les centraux téléphoniques IP ont peu à peu pris la place de leur ancêtres analogiques dans les entreprises quelle que soit leur taille qui, connectées à Internet, abaissent le coût de leurs communications et celui de l'entretien de l'infrastructure téléphonique. Ceci est aussi dû à la convergence physique des réseaux de données et téléphoniques qui empruntent désormais des routes communes.

Les systèmes de téléphonie sur IP héritent aussi de toutes les menaces et vulnérabilités qui dégradent régulièrement le fonctionnement des réseaux informatiques. De plus, les agissements de personnes ou d'organisation hostiles et malveillantes sont facilités dans le domaine notamment des écoutes et autres indiscrétions. Toutefois, les protections disponibles sur les réseaux de données profitent directement aux réseaux téléphoniques qui ont à leur disposition un arsenal complet de mesures parmi lesquelles la cryptographie tient une place de choix.

© ENI Editions - All rigths reserved - Moha Anisa

Généralités et historique

Les pare-feu ou firewalls sont apparus et ont connu leur heure de gloire lorsque les réseaux d'entreprise se sont progressivement vus connectés à Internet, ce réseau qui a toujours été perçu comme une menace. D'une manière générale, les firewalls protègent les réseaux internes des réseaux extérieurs et cet état de fait est toujours de mise aujourd'hui. Les architectures évoluant, les firewalls tout en restant à leur place originelle investissent l'intérieur du réseau. Les modes de travail tendent vers une étroite imbrication des acteurs qui gravitent autour du système d'information et il est devenu courant de fournir à des partenaires l'accès à des ressources internes. Cette situation entraîne un tel bouleversement dans les architectures de sécurité (et réseau) qu'une réflexion s'impose afin de redéfinir les nouvelles limites et les nouvelles règles de sécurité encadrant un trafic toujours plus dense et plus complexe au profit des applications qu'il véhicule.

Les firewalls trouvent toujours leur place dans cette redistribution des cartes et leurs capacités se sont au fil des années étoffées avec l'apparition de fonctionnalités devenues indispensables parmi lesquelles figurent l'authentification des utilisateurs, les VPN SSL et la surveillance des protocoles applicatifs. Toutefois, les firewalls accomplissent toujours le filtrage des protocoles réseau qui est à l'origine de leur création.

Nous allons dans ce chapitre brosser un portrait des fonctionnalités proposées par les firewalls en débutant par leurs missions premières (le filtrage IP) jusqu'aux derniers développements (les VPN SSL). Nous avons choisi pour illustrer notre propos le modèle ASA 5505 qui est le firewall d'entrée de gamme de Cisco au moment de l'écriture de ce livre.

Cisco s'est illustré dans le domaine du firewall avec le célèbre modèle PIX (*Private Internet Exchange*) livré dès ses débuts sous la forme d'un équipement compact et fiable libérant l'administrateur des contraintes de gestion d'un système d'exploitation sous-jacent. Tel n'était pas le cas des autres firewalls quasi exclusivement conçus pour être installés sur des plates-formes Unix ou Windows. La gamme PIX s'est éteinte en 2008. Elle est remplacée par la gamme ASA (*Adaptive Security Appliances*) qui perpétue la tradition des équipements dédiés et autonomes.

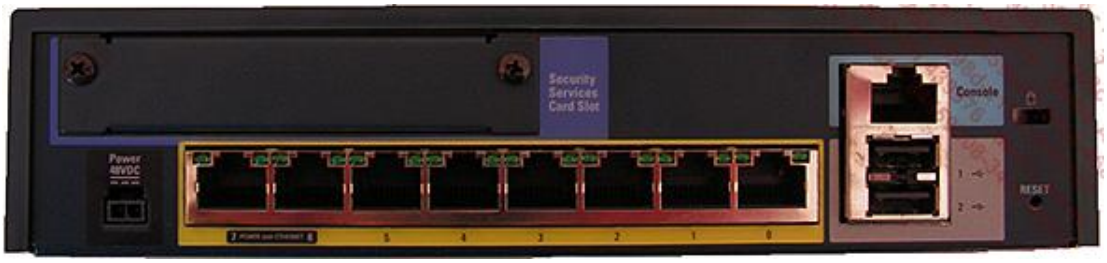
Cette nouvelle famille fait la part belle aux techniques émergentes comme les VPN SSL qui ont pour vocation de remplacer les tunnels VPN basés sur IPSec dédiés aux utilisateurs distants. Le but avoué de cette technologie est de faciliter l'accès (sécurisé) aux applications publiées au format WEB à tous les employés et partenaires de l'entreprise en fonction de rôles préalablement définis et finement attribués. Le firewall est devenu ainsi au-delà de sa fonction de filtrage réseau une véritable passerelle multi niveau assurant des services d'accès et de sécurité sur toute l'étendue du modèle OSI.

© ENI Editions - All rigths reserved - Moha Anisa

Présentation de l'ASA 5505

Le firewall ASA 5505 est présenté sous la forme d'un petit boîtier dont les dimensions le place parmi les plus compacts du marché : 20 cm x 17cm x 4.5 cm. Il est principalement destiné aux petites et moyennes entreprises, aux télétravailleurs ainsi qu'aux agences de taille modeste. Ses possibilités en revanche sont proches de celles des modèles supérieurs. Toutefois, les fonctions de haute disponibilité ne sont pas offertes (avec la licence de base) et le nombre de VLAN gérés est limité. Il n'est également pas possible d'exploiter la technologie des contextes de sécurité qui autorise la création de multiples instances de firewall virtuelles au sein d'un même équipement physique. Le Firewall ASA 5505 est un équipement d'entrée de gamme relativement limité dans ses capacités de configuration réseau par rapport aux modèles supérieurs. Il est en revanche administré avec un outil très évolué.

La face avant du boîtier comporte des LED indiquant l'état de l'équipement et des connexions réseau. Le port USB n'est pas utilisé.



Sur la face arrière nous trouvons les huit ports d'un commutateur Ethernet qui ont la possibilité d'être organisés en trois VLAN locaux. Le port zéro est par défaut réservé à l'interface externe connectée au réseau le moins sûr. Les sept autres ports sont considérés comme étant internes au réseau. Les deux derniers ports offrent une alimentation électrique afin d'alimenter un poste téléphonique IP. Le connecteur de la console est entouré de bleu et les deux ports USB sont réservés à de futures applications. Un emplacement est réservé pour accueillir une carte d'extension qui prend en charge un module dédié à l'inspection virale. Sur la droite du port console, la petite fente permet d'attacher le firewall à un support à l'aide d'un câble de sécurité du même type que ceux utilisés pour les ordinateurs portables.

Cisco annonce une capacité de traitement de 150 Mbps par le firewall et 100 Mbps lorsque le chiffrement est activé. En fonction des licences, le firewall est limité en nombre d'utilisateurs normaux ou utilisant les connexions protégées de type VPN IPSec ou VPN SSL.

1. Configuration de base

Nous présentons la configuration du firewall ASA en nous basant principalement sur la ligne de commande (CLI). L'interface graphique d'administration ASDM sera présentée en annexe.

Le firewall est livré avec une configuration de base qui comporte deux interfaces routées. Ce sont des interfaces VLAN identiques à celles des commutateurs de la gamme. Chacune d'entre elle reçoit une désignation qui est reprise par exemple dans les commandes de traductions d'adresse.

Les deux interfaces VLAN de la configuration de base sont nommées *inside* et *outside*. Chacune d'elle est associée à un niveau de sécurité.

```
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.2.1 255.255.255.0
```

© ENI Editions - All rigths reserved - Moha Anisa

```
!
```

Dans cet extrait de configuration, nous remarquons la commande `nameif` qui donne son appellation aux deux interfaces. La commande `security-level` est quant à elle suivie d'une valeur qui indique son niveau de sécurité. Plus le chiffre est grand et plus l'interface est digne de confiance tout comme les réseaux qui y sont connectés (cent est le maximum).

Il faut retenir que par défaut, le trafic transite uniquement entre deux interfaces du niveau le plus élevé vers le niveau le moins élevé. Dans l'extrait de configuration ci-dessus, les membres du VLAN 1 (qui représente l'intérieur du réseau) peuvent initialiser des connexions vers le VLAN 2 (qui représente l'extérieur du réseau). Pour déroger à cette règle de base l'utilisation d'une ACL est indispensable.

Une spécificité de l'ASA 5505 livré avec une licence de base est l'obligation de rendre unidirectionnel le trafic entre deux des trois interfaces VLAN qu'il est possible de créer. Si l'on décide de configurer trois interfaces de type VLAN. Le message suivant apparaît alors :

```
ERROR: This license does not allow configuring more than 2
interfaces with nameif and without a "no forward" command on this
interface or on 1 interface(s)
```

Ce message nous met en garde et indique qu'il faut limiter le trafic entre deux des trois interfaces.

```
interface Vlan3
 no forward interface Vlan1
 nameif DMZ
 security-level 50
```

Ici, l'interface VLAN3 est configurée de telle sorte qu'elle ne puisse pas initialiser de communication vers l'interface VLAN1. D'autre part, son niveau de sécurité est de 50 ce qui la situe entre les valeurs des deux autres interfaces.

```
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
 switchport access vlan 3
```

Les interfaces physiques du commutateur Ethernet intégré dans l'ASA sont au final raccordées aux divers VLAN en utilisant la commande `switchport access vlan` suivie bien entendu d'un numéro de VLAN. Pour ce faire, il faut utiliser le mode de configuration d'une interface physique. Les interfaces dans le VLAN1 n'apparaissent pas dans le rappel de configuration.

Tout comme pour les autres équipements, le firewall ASA dispose du protocole SSH afin de sécuriser les accès administratifs.

```
ASA-5505(config)# domain-name testlab.com
ASA-5505(config)# crypto key generate rsa modulus 2048
ASA-5505(config)# username vincent password cisco
ASA-5505(config)# aaa authentication ssh console LOCAL
ASA-5505(config)# ssh 192.168.1.2 255.255.255.255 inside
ASA-5505(config)# ssh timeout 5
ASA-5505(config)# ssh version 2
ASA-5505(config)# management-access inside
```

Cet extrait de configuration est relativement explicite. Notons toutefois la simplification en comparaison avec un routeur. Ici, les interfaces VTY ont disparu. Il est simplement indiqué au protocole SSH l'adresse IP de la station d'administration et l'interface VLAN sur laquelle ce trafic aboutit. Il s'agit en l'occurrence de l'interface *inside* qui correspond à l'interface VLAN1.

```
username vincent password Vtb/ZufSkY.w0v3m encrypted privilege 15
```

Le compte local (utilisateur vincent) vu après un rappel de la configuration montre ici son mot de passe chiffré et son niveau de privilège.

© ENI Editions - All rigths reserved - Moha Anisa

Exigences de sécurité

Nous avons évoqué la place des firewalls dans l'architecture réseau en insistant sur le fait qu'elle ne se limite plus uniquement aux frontières traditionnelles. Des services hautement sensibles comme la téléphonie, bien qu'hébergés à l'intérieur du périmètre, nécessitent une protection accrue afin que rien d'autre que les protocoles associés à la voix ne pénètre dans la zone des serveurs dédiés à la voix. Il en va de même pour d'autres zones applicatives. Toutefois, les firewalls ne quitteront sans doute jamais les emplacements qui marquent la séparation du réseau d'une entreprise avec le monde extérieur.

La valeur ajoutée des premiers équipements de filtrage était bien faible malgré l'adjonction des services de traduction d'adresses devenus indispensable avec l'avènement d'Internet et les menaces qu'il ne manque pas de charrier. C'est pourquoi, les éditeurs de firewalls les ont dotés de fonctionnalités plus évoluées qui concentrent sur un équipement unique des fonctions annexes comme l'authentification des utilisateurs et la surveillance approfondie des protocoles applicatifs.

Nous avons examiné au cours du chapitre La sécurité de la couche réseau la configuration sur un routeur de la suite IPSec qui est initialement destinée aux communications de réseau à réseau. Cette technique couramment nommée VPN est également applicable à la relation entre un individu (sa station de travail) et un réseau central. Elle nécessite l'installation d'un client lourd accompagné de réglages spécifiques de la suite IPsec et de la couche réseau. Partant du principe qu'une station de travail possède un navigateur Internet disposant de fonction cryptographique, des solutions sont apparues qui utilisent les fonctions SSL du navigateur en substitution de celle d'un client lourd. Les accès au réseau central sont de fait envisageables depuis n'importe quelle station de travail ce qui pose, nous le verrons, quelques problèmes.

Ce sont ces techniques que nous allons décrire mais auparavant, définissons comme de coutume des exigences de sécurité par rapport aux fonctionnalités que nous venons d'évoquer.

Exigences de sécurité Firewall pour les fonctions de filtrage IP	
Filtrage IP avec conservation de l'état des sessions	ACL
Implémentation de DMZ	Configuration
Traduction d'adresse et protection des serveurs publics	NAT
Détection et protection contre les menaces au sein des protocoles applicatifs	Service d'inspection des protocoles applicatifs

1. Les ACL

Bien entendu le firewall ASA possède la capacité de garder en mémoire l'état des sessions en cours. Comme nous l'avons décrit lors du chapitre sur la sécurité au niveau 3, le firewall autorise le trafic retour correspondant à celui défini sur l'ACL.

La terminologie des ACL diffère légèrement de celle en vigueur sur les routeurs, il est également possible de déclarer (grouper) des réseaux, des équipements, des protocoles et des services pour les intégrer à la configuration de l'ACL. L'application de l'ACL à l'interface ne s'effectue pas dans le mode de celle-ci.

```
ASA-5505(config)# object-group ?

configure mode commands/options:
  icmp-type  Specifies a group of ICMP types, such as echo
  network    Specifies a group of host or subnet IP addresses
  protocol   Specifies a group of protocols, such as TCP, etc
  service    Specifies a group of TCP/UDP ports/services
```

```
ASA-5505(config)# object-group network inside
ASA-5505(config-network)# ?

  description     Specify description text
  group-object    Configure an object group as an object
  help         Help for network object-group configuration commands
  network-object  Configure a network object
  no              Remove an object or description from object-group
```

© ENI Editions - All rigths reserved - Moha Anisa

```
ASA-5505(config-network)# network-object 192.168.4.0 255.255.255.0
ASA-5505(config-network)# network-object 192.168.5.0 255.255.255.0
ASA-5505(config-network)# network-object 192.168.6.0 255.255.255.0
```

Ces trois captures de configuration montrent les étapes de la création de trois objets désignant chacun un réseau. Nous créons un groupe d'objets (`object-group`) de type `network` portant le nom `inside`. Puis, nous associons trois objets réseaux à ce groupe. Le but est de désigner sous un nom unique trois réseaux interieurs qui ne sont pas directement connectés à l'interface interne.

```
object-group network inside
 network-object 192.168.4.0 255.255.255.0
 network-object 192.168.5.0 255.255.255.0
 network-object 192.168.6.0 255.255.255.0
```

Cet extrait de la configuration montre plus explicitement le regroupement des trois réseaux.

```
ASA-5505(config)# access-list ACL-Interne extended permit ip
object-group inside any
ASA-5505(config)#  access-group ACL-Interne in interface inside
```

La première des deux commandes ci-dessus crée une ACL et la nomme `ACL-Interne` de type étendue et sélectionne le groupe d'objets nommé `inside` comme source du trafic IP et à destination de n'importe quelle direction.

La seconde commande applique l'ACL en entrée (`in`) sur l'interface `inside`.

```
ASA-5505(config)# access-list ACL-Interne line 2 deny ip
192.168.9.0 255.255.255.0
```

À la manière de ce qui existe pour les routeurs il est possible de numéroter les entrées d'une ACL afin de faciliter l'inclusion d'une nouvelle ligne dans la liste.

```
ASA-5505(config)# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max
4096)
            alert-interval 300

access-list ACL-Interne; 5 elements
access-list ACL-Interne line 1 extended permit ip object-group
inside any 0x4d17491e
access-list ACL-Interne line 1 extended permit ip 192.168.4.0
255.255.255.0 any (hitcnt=0) 0x6b96d490
access-list ACL-Interne line 1 extended permit ip 192.168.5.0
255.255.255.0 any (hitcnt=0) 0xf64614a7
access-list ACL-Interne line 1 extended permit ip 192.168.6.0
255.255.255.0 any (hitcnt=0) 0x4ac0eade
access-list ACL-Interne line 2 extended deny ip 192.168.9.0
255.255.255.0 any (hitcnt=0) 0x60adaa36
```

Le retour de la commande `show access-list` nous montre la ligne 1 qui fait référence au groupe d'objets nommé `inside`. Puis, nous observons la ligne 2 qui interdit le réseau 192.168.9.0. Si l'on souhaite intercaler une ligne entre la ligne 1 et la ligne 2, il suffit de créer une nouvelle ligne 2. L'ancienne ligne 2 devient alors la ligne 3.

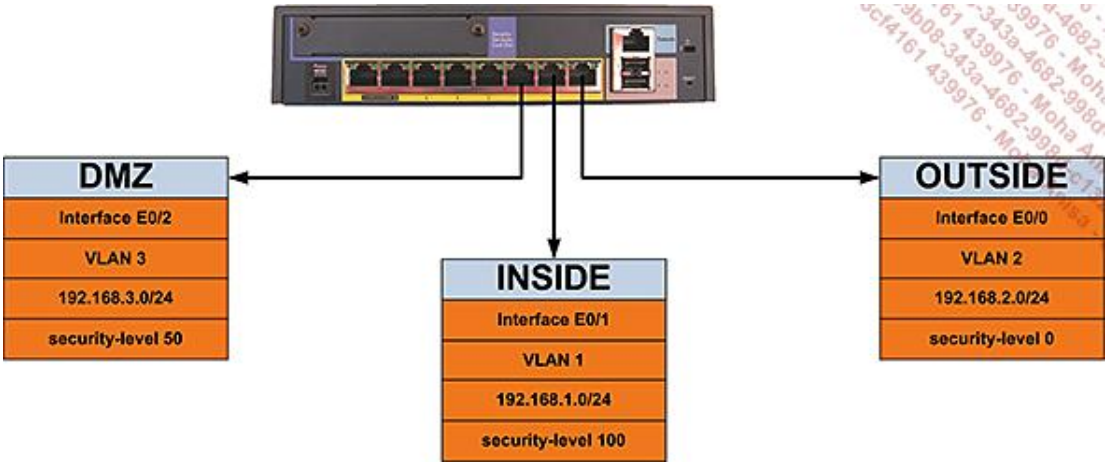
2. Les DMZ et NAT

Nous allons aborder deux notions qui sont étroitement liées sur tous les réseaux sécurisés, ce sont la création de zones démilitarisées (DMZ) et l'utilisation de la traduction d'adresse (NAT).

La combinaison de ces deux techniques et l'appui des ACL permettent :

- de masquer le réseau interne à la vue du monde extérieur ;
- de créer une zone de sécurité intermédiaire entre l'intérieur et l'extérieur ;
- de publier des informations dans cette zone en la rendant accessible de l'extérieur.

© ENI Editions - All rigths reserved - Moha Anisa



Voici une représentation d'un firewall ASA 5505 sur lequel trois zones sont créées. Les interfaces physiques Ethernet 3 à 7 sont par défaut rattachées au VLAN1 et font partie de la zone INSIDE (intérieure).

Il existe une règle d'or concernant les DMZ, celle qui recommande de ne pas laisser une zone initialiser des communications vers une zone dont le niveau de sécurité est supérieur au sien. C'est le principe du moindre privilège.

Cette règle appliquée par défaut à nos trois interfaces par le firewall est résumée dans ce tableau. Il existe cependant des cas de figure pour lesquels les communications doivent s'établir afin d'alimenter la zone DMZ en informations. Ces communications devraient débuter à partir de la zone INSIDE vers la zone DMZ. Il est parfois opportun d'interdire au trafic de s'écouler dans le sens qui est autorisé par défaut. Si nous considérons la zone DMZ munie d'un serveur WEB, nous pouvons soulever la question de l'utilité pour cette zone d'établir des communications avec l'extérieur. En effet, ce type de serveur renvoie vers l'extérieur des informations et ne communique jamais de sa propre initiative vers l'extérieur. Ce n'est par contre pas le cas des serveurs de messagerie. Un autre cas d'application de cette règle interdirait à la zone OUTSIDE de contacter la DMZ sur laquelle sont déployés des services à vocation publique. Il apparait clairement que l'organisation des flux (vue sous l'aspect sécurité) ne relève pas uniquement de la nature de la zone d'origine malgré le bien fondé du principe du moindre privilège. Afin de déroger à cette règle implémentée par défaut sur les Firewall ASA (avec les niveaux de sécurité), il faut déployer des ACL. Elles seules sont à même d'autoriser de manière granulaire des accès qui sont interdits par défaut.

La création de DMZ sur le firewall ASA s'opère par la configuration du niveau de sécurité des interfaces VLAN. Le schéma représente l'exemple type dans lequel la zone interne (INSIDE) reçoit la valeur de 100, la zone externe (OUTSIDE) la valeur minimale de 0, la DMZ quant à elle reçoit la valeur intermédiaire de 50.

Avec cette configuration, nous obtenons par défaut le tableau suivant qui respecte le principe de moindre privilège.

	vers INSIDE	**vers DMZ**	**vers OUTSIDE**
de INSIDE	OK	OK	OK
de DMZ	NON	OK	OK
de OUTSIDE	NON	NON	N/A

Au début d'Internet, les équipements terminaux recevaient tous une adresse publique. Ils étaient de fait directement joignables. Ce n'est plus le cas de nos jours où la plupart des systèmes terminaux utilisent des adresses dites privées masquées (NAT) par une ou plusieurs adresses publiques. Nous allons décrire les deux cas les plus courants, il s'agit de la connexion d'un réseau privé à Internet et de la mise à disposition d'un service public sur une DMZ avec un adressage privé. Ces cas sont des classiques du genre, mais ont pour mérite d'aider grandement à la compréhension de cette technique.

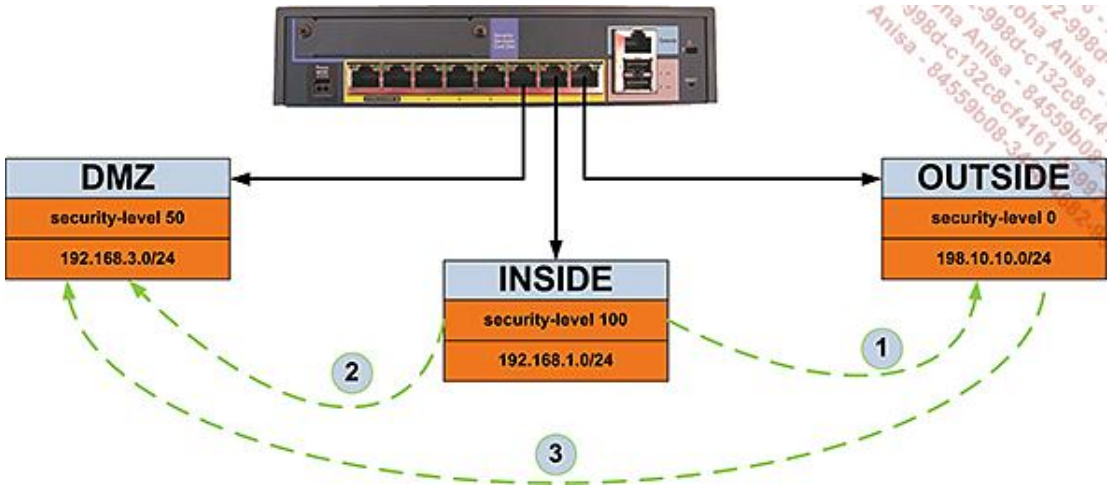
NAT (*Network Address Translation*) est considéré comme une fonction de sécurité à part entière car ses caractéristiques permettent une isolation entre les réseaux publics et privés. NAT est apparu avec la nécessité d'économiser les adresses IP publiques d'Internet. De plus, il est rapidement devenu inconcevable en matière de sécurité de laisser un ordinateur directement connecté à Internet. Des plages d'adresses IP ont été déclarées non routables (donc inutilisables) sur Internet et mise à disposition des entreprises pour un usage interne. Ces plages d'adresses sont connues sous l'appellation RFC 1918 et sont :

- 10.0.0.1 à 10.255.255.254 ;
- 172.16.0.1 à 172.31.255.254 ;

© ENI Editions - All rigths reserved - Moha Anisa

- 192.168.0.1 à 192.168.255.254.

NAT modifie les champs source ou destination des paquets IP au passage de ces derniers sur le firewall. Dans les cas qui suivent, nous utiliserons NAT pour modifier l'adresse source des paquets IP sortant du réseau INSIDE vers le réseau OUTSIDE et pour modifier l'adresse destination des paquets IP en provenance du réseau OUTSIDE vers le réseau DMZ.

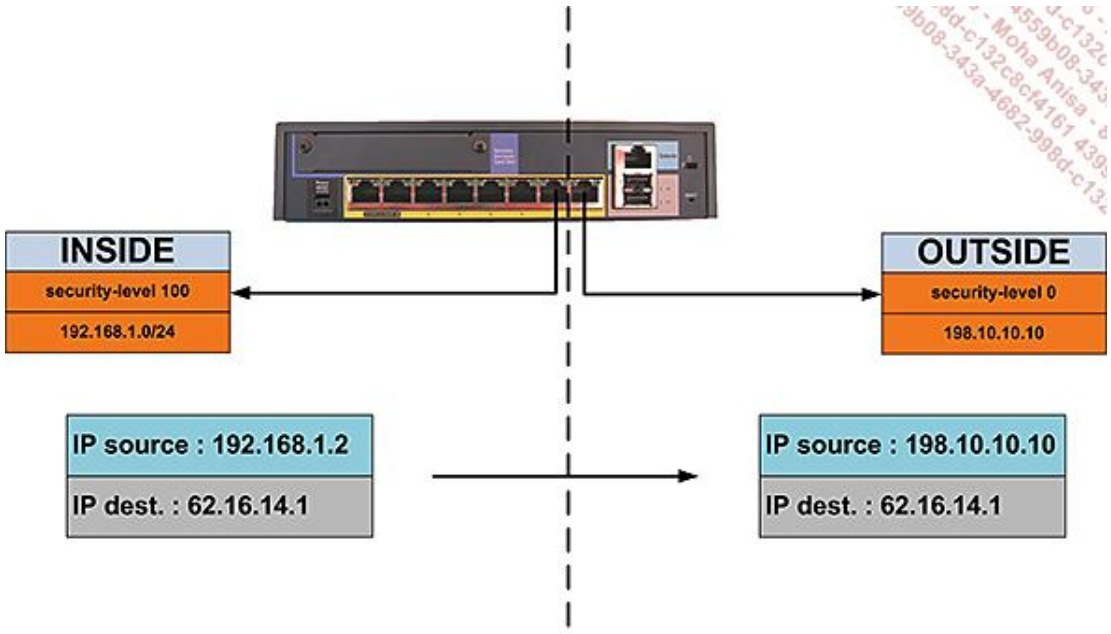


Nous montrerons également comment ne pas utiliser NAT entre le réseau INSIDE et le réseau DMZ.

Nous allons décrire les trois cas les plus courants, il s'agit (en 1) de la connexion du réseau INSIDE au réseau OUTSIDE, de la connexion (en 2) du réseau INSIDE vers le réseau DMZ et de la connexion (en 3) du réseau OUTSIDE vers la DMZ. Ces trois configurations utilisent la traduction d'adresse et les ACL.

Cas N° 1 :

Le réseau INSIDE se connecte au réseau OUTSIDE. Ce cas montre une station de travail d'un réseau interne qui se connecte sur Internet. Comme elle ne dispose pas d'une adresse publique (routable sur Internet) il est absolument nécessaire de changer l'adresse IP source des paquets IP. Si tel n'était pas le cas, les paquets retour ne pourraient trouver leur destination.



Lors de son passage à travers le firewall le paquet IP change d'adresse source. Son adresse de type RFC 1918 est transformée en adresse IP publique, en l'occurrence celle de l'interface `outside`. Aucune ACL n'est ici nécessaire car le réseau INSIDE bénéfice du niveau de sécurité maximal. Cet exemple montre le réseau INSIDE en correspondance avec l'adresse de l'interface OUTSIDE du firewall.

```
ASA-5505(config)# nat (inside) 1 192.168.1.0 255.255.255.0
ASA-5505(config)# global (outside) 1 interface
```

La syntaxe des commandes NAT n'est pas facile à retenir et mérite des explications approfondies.

© ENI Editions - All rigths reserved - Moha Anisa

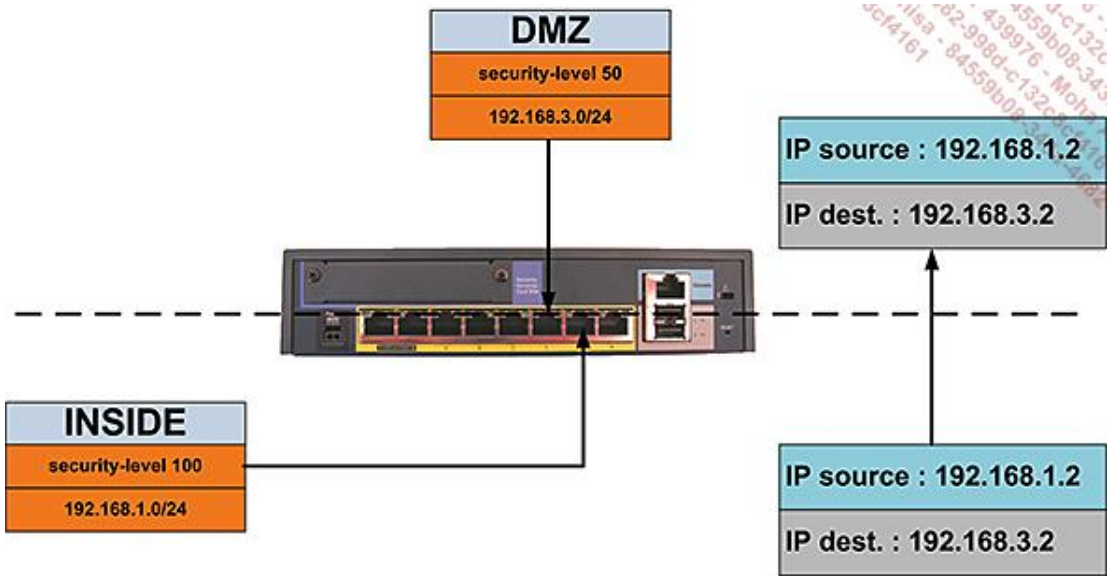
Ici, nous déclarons un processus NAT qui porte le numéro 1. Il est indiqué que le réseau 192.168.1.0 résidant sur l'interface `inside` (commande `nameif` de l'interface VLAN1) est candidat pour la transformation des adresses sources (`nat`) au passage du firewall vers le réseau `outside` qui se situe en zone publique (`global`). Les deux lignes sont liées par le numéro 1. Lors du passage d'un paquet, la table de correspondance de NAT est renseignée afin de permettre la distribution correcte du paquet retour.

```
ASA-5505(config)# nat (inside) 1 192.168.1.0 255.255.255.0
ASA-5505(config)# global (outside) 1 198.10.10.10-198.10.10.240
```

Il est également possible de faire correspondre le réseau INSIDE à un groupe d'adresses publiques routées sur l'interface OUTSIDE. Dans cet extrait de configuration, aux adresses du réseau INSIDE correspondent une plage d'adresses publiques c'est-à-dire toutes les adresses entre 198.10.10.10 et 198.10.10.240

Cas N° 2 :

Faut-il activer les fonctions NAT pour tous les types de trafic ? Cela ne paraît pas indispensable entre deux réseaux qui possèdent des adresses IP privées. Le cas se présente dans notre architecture pour les communications entre le réseau INSIDE et le réseau DMZ. Le cas N°1 transforme toutes les adresses du réseau INSIDE. Si la fonction NAT n'est pas nécessaire entre le réseau INSIDE et le réseau DMZ, il faut indiquer au processus NAT qu'il ne doit pas traiter certains paquets.



Nous observons ici que les paquets entre le réseau INSIDE et le réseau DMZ conservent leur adresse source.

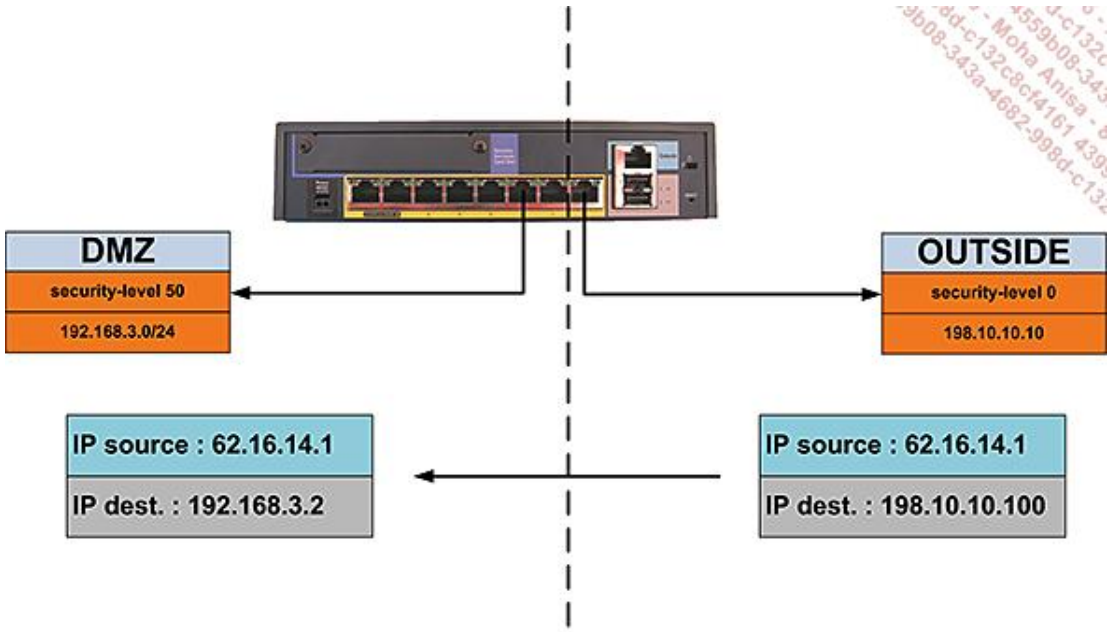
```
ASA-5505(config)# access-list PasDeNat permit ip 192.168.1.0
255.255.255.0 192.168.3.0 255.255.255.0

ASA-5505(config)# nat (inside) 0 access-list PasDeNat
```

Une ACL (nommée PasDeNat) désigne le trafic entre le réseau INSIDE et le réseau DMZ. Puis, cette ACL est appliquée à une commande NAT s'appliquant sur l'interface `inside` suivie du chiffre 0 indiquant qu'il ne faut pas transformer les adresses sources correspondant à l'ACL PasDeNat.

Cas N° 3 :

Les services offerts au public sont généralement installés sur des zones démilitarisées afin de bénéficier de la protection offerte dans ces espaces. La traduction d'adresse est l'une de ces protections. Il faut que le serveur dans le réseau DMZ soit accessible de l'extérieur par son adresse publique. Puis NAT modifie l'adresse de destination publique vers l'adresse privée du serveur telle que configurée sur sa carte réseau. En outre, cette communication s'établit entre l'interface `outside` (security-level 0) et l'interface `dmz` (security-level 50) ce qui nécessite l'ajout d'une ACL pour déroger au principe du moindre privilège.

© ENI Editions - All rigths reserved - Moha Anisa



Nous constatons le changement du champ IP destination dans le paquet lors du passage au travers du firewall. Cette configuration nécessite un routage de l'adresse 198.10.10.100 sur l'adresse de l'interface `outside`.

```
static (inside,outside) 198.10.10.100 192.168.3.2 netmask
255.255.255.255

access-list VersDMZ extended permit tcp host 198.10.10.100 eq www
host 192.168.3.2 eq www

access-group VersDMZ in interface outside
```

Ces deux commandes décrivent :

- l'association entre l'adresse publique du serveur (198.10.10.100) et son adresse privée (192.168.3.2) ;
- l'indispensable ACL pour passer d'un niveau de sécurité à l'autre. Examinons-les dans le détail.

La première commande n'est pas aisée à mémoriser de prime abord. Elle indique au routeur qu'une adresse IP du côté de l'interface `inside` est statiquement traduite sur l'interface `outside` par NAT. Nous trouvons ensuite l'adresse IP publique du serveur suivie de son adresse privée. Cette syntaxe est quelque peu déroutante du fait de l'inversion des adresses par rapport à l'ordre des mots `inside` et `outside`.

La seconde commande est une ACL étendue classique qui autorise l'adresse publique du serveur à se connecter à son adresse privée, les ports sont précisés et correspondent au protocole HTTP (port 80).

Des contrôles supplémentaires existent pour les règles de traduction et concernent la couche session. Il est possible de configurer un nombre maximum de connexions TCP et UDP. La quantité de connexions à moitié ouvertes est également configurable.

3. Détection et protection contre les menaces

Les attaques portant sur les protocoles du réseau ne manquent pas. Elles s'échelonnent de la simple reconnaissance de port à la mise hors service d'un réseau par l'envoi en grand nombre de paquets volontairement erronés. Les attaques de ce genre peuvent tout à fait traverser un firewall si elles correspondent à du trafic autorisé. Il peut sembler irréaliste d'enregistrer dans les journaux ces trafics légitimes, mais une brutale augmentation d'une catégorie de trafic est une information de premier choix hélas noyée dans le flux incessant qui traverse un équipement de sécurité. Ce principe est séduisant mais induit pour un firewall, aussi doté en mémoire soit-il, une charge de travail considérable. Il est préférable de déléguer à d'autres outils le soin de surveiller la charge des liens du réseau voire la conformité applicative du trafic. Parmi ces outils nous trouvons les dispositifs de corrélation de journaux qui présentent un avantage incontestable en comptabilisant les occurrences d'un même évènement au lieu de créer une ligne pour chacun d'entre eux.

Après la détection d'une activité paraissant suspecte, il convient de prendre une décision quant au traitement du trafic incriminé. Il est envisageable de l'éliminer totalement ou de restreindre son taux de pénétration dans le réseau

© ENI Editions - All rigths reserved - Moha Anisa

par le biais des outils de qualité de service.

Nous avons examiné sur les routeurs des ACL qui permettent de rejeter sur les interfaces externes, du trafic semblant provenir des réseaux internes. De même, nous avons souligné l'intérêt représenté par un filtrage à la source au plus près des connexions des utilisateurs.

Nous allons à présent examiner les solutions proposées sur le firewall ASA.

Le taux de messages de sécurité concernant le nombre de paquets rejetés par des ACL est tout particulièrement intéressant car il indique une anomalie due ou non à une attaque sur le réseau.

```
ASA-5505(config)# threat-detection basic-threat
```

Cette première commande active la détection des menaces sur une liste prédéterminée d'irrégularité comme les rejets sur les ACL, un nombre trop important de paquets SYN en attente de synchronisation ou une reconnaissance par scan de ports. Un message est enregistré sur le journal du firewall. Les taux de détection sont très facilement paramétrables et portent sur la durée pendant laquelle seront calculées les moyennes, le taux moyen de paquets rejetés par seconde et un taux de pic sur un intervalle plus court. Ces commandes ne présentent aucune difficulté particulière mais nécessitent un paramétrage réaliste en fonction des seuils souhaités.

```
hostname(config)# threat-detection rate {acl-drop | bad-packet-drop
| conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop
|interface-drop | scanning-threat |
syn-attack} rate-interval rate_interval average-rate av_rate burst-
rate burst_rate
threat-detection rate syn-attack rate-interval 1200 average-rate
100
```

Le détail de la commande est donné pour information. Nous trouvons au-dessous, une commande visant à remonter une alerte en cas de dépassement d'un certain réglage dans le cas d'une attaque par inondation de paquets SYN. Après chaque mot clé et avant chaque valeur en secondes, l'utilisation du point d'interrogation fournit (en anglais) des explications très détaillées sur l'utilisation de chaque mot clé. Cette aide en ligne est d'une très grande qualité. La commande en exemple se traduit de la manière suivante : le taux de détection des menaces pour une attaque SYN (présumée) est calculé sur un intervalle de 1200 secondes et déclenche une alarme pour un taux de 100 paquets par seconde.

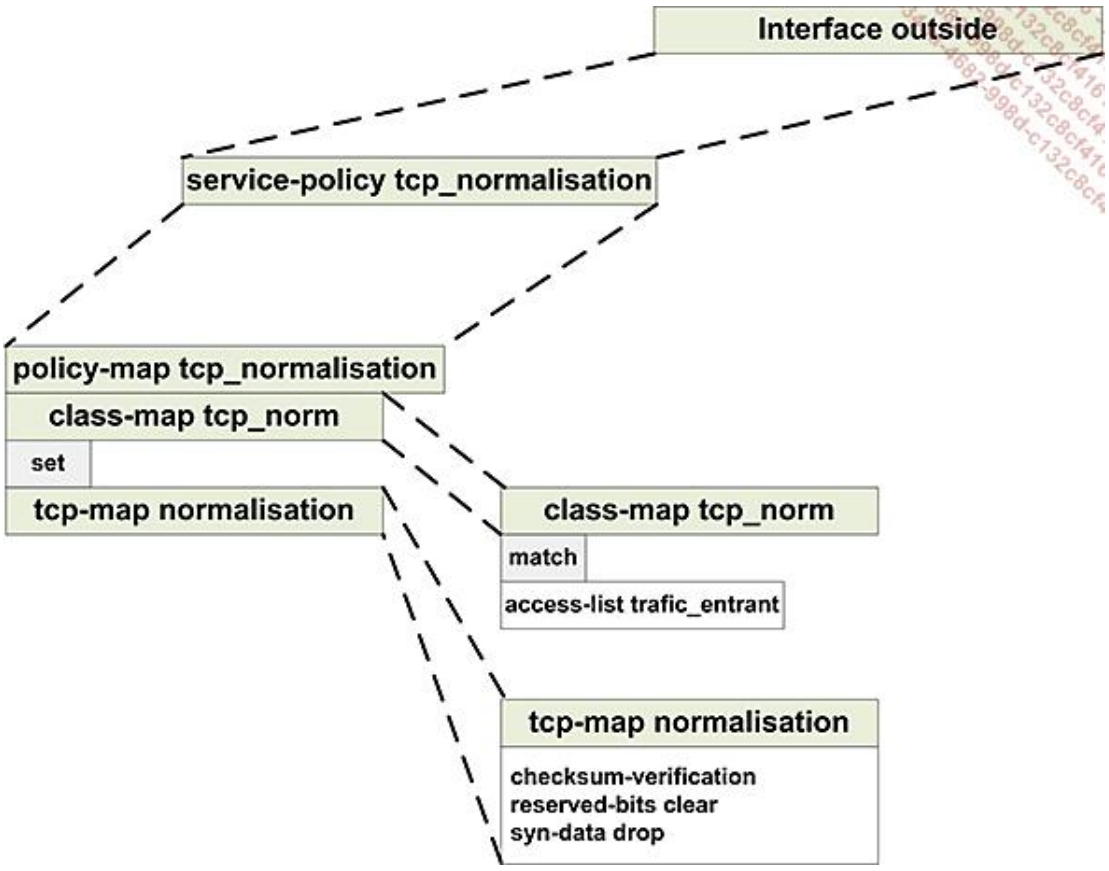
```
ASA-5505(config)# threat-detection scanning-threat shun duration 60
```

Cette autre commande concerne plus particulièrement les reconnaissances par scan de port. Il est ici question non seulement de remonter un message en cas de reconnaissance mais aussi de déconnecter le gêneur pour une durée d'une minute grâce à l'option `shun` qui est optionnelle. Pour mémoire une reconnaissance est un nombre considérable de tentatives de connexions sur tous les ports connus afin de déterminer quels sont ceux sur lesquels le système d'exploitation visé est en écoute.

Cisco sous l'appellation de « normalisation du protocole TCP » offre une myriade d'options très intéressantes pour tenter de paramétrer finement la détection des attaques dont TCP est la victime. Ici aussi le point d'interrogation apporte beaucoup d'informations. Citons toutefois quelques options portant sur la détection des drapeaux ACK ou URGENT mal positionnés ainsi que la possibilité d'accepter une variation de la taille des fenêtres.

Le mécanisme d'application de la normalisation du protocole TCP à une interface suit le schéma utilisé pour ajuster la qualité de service. La syntaxe utilisée par Cisco est « à tiroir » et mérite que l'on s'y arrête quelques instants.

© ENI Editions - All rigths reserved - Moha Anisa



Tout d'abord, nous définissons les paramètres de normalisation (en bas à droite), puis une `class-map` est créée dans laquelle le trafic défini par une ACL est sélectionné pour la normalisation. Tout ceci est intégré dans une `policy-map` (qui peut contenir plusieurs entrées `class-map` et `set`). Pour terminer, une `service-policy` englobe la `policy-map` avant de se voir affectée à l'interface `outside`.

```
ASA-5505(config)# access-list trafic_entrant extended permit tcp
any host 198.10.10.100 eq www

ASA-5505(config)# tcp-map normalisation
ASA-5505(config-tcp-map)# checksum-verification
ASA-5505(config-tcp-map)# reserved-bits clear
ASA-5505(config-tcp-map)# syn-data drop
ASA-5505(config-tcp-map)# exit

ASA-5505(config)# class-map tcp_norm
ASA-5505(config-cmap)# match access-list trafic_entrant
ASA-5505(config-cmap)# exit

ASA-5505(config)# policy-map tcp_normalisation
ASA-5505(config-pmap)# class tcp_norm
ASA-5505(config-pmap-c)# set connection advanced-options
normalisation

ASA-5505(config-pmap-c)# exit
ASA-5505(config-pmap)# exit

ASA-5505(config)# service-policy tcp_normalisation interface
outside
ASA-5505(config)#
```

Cette capture comporte la totalité des commandes qui correspondent au schéma d'organisation de cette configuration en cascade. Nous touchons ici aux séquences de commandes parmi les plus complexes introduites par Cisco.

4. Où l'on reparle de la téléphonie sur IP

© ENI Editions - All rigths reserved - Moha Anisa

Le firewall ASA offre des mesures de sécurité pour la téléphonie sur IP parmi lesquelles nous retiendrons la possibilité de déchiffrer à la volée la signalisation afin de l'inspecter (*TLS-proxy*), l'inspection protocolaire proprement dite et la fonction *phone proxy*.

a. TLS-proxy

TLS-proxy place le pare-feu en coupure entre un téléphone et le CUCM afin de « défaire et refaire » la session TLS qui protège la signalisation. Une fois en clair, la signalisation est inspectée puis chiffrée à nouveau avant d'être redirigée vers le CUCM. Cette architecture nécessite la mise en place d'un certificat sur le pare-feu à la manière de celui présent sur le CUCM et la mise à jour de la liste de confiance présente sur le téléphone. TLS-proxy nécessite l'installation de certificats sur le pare-feu afin de représenter le CUCM pour les téléphones et une mise à jour de leur liste de sécurité interne.

b. Inspection protocolaire

Il est ici question de vérifier la conformité du protocole de signalisation par rapport à des règles définies dans la configuration du pare-feu. Ces règles seront confrontées à la signalisation. L'inspection du protocole vérifie également les propriétés TCP de la connexion et offre l'opportunité de rendre aléatoire les numéros de séquences. Enfin, une règle de qualité de service peut aussi être appliquée au trafic (en l'occurrence la signalisation).

```
class-map VoIP
 match any
!
policy-map type inspect skinny Inspection-SCCP
 parameters
  enforce-registration
  message-id max 0x141
  sccp-prefix-len max 65536
  timeout media 0:01:00
  timeout signaling 0:05:00
  rtp-conformance enforce-payloadtype
policy-map global-policy
 description Telephonie
 class VoIP
  inspect skinny Inspection-SCCP
  set connection conn-max 100 embryonic-conn-max 20 per-client-max
3
  set connection timeout tcp 1:00:00 reset dcd 0:15:00 5
  set connection decrement-ttl
!
service-policy global-policy global
```

Cet extrait montre la configuration de la protection du protocole SCCP. Le schéma consiste à déclarer un *policy-map* de type *inspect* puis à l'insérer dans une *policy-map* nommée *global-policy*. Cette dernière est appelée dans une commande `service-policy` appliquée globalement (`global`). La *class-map* nommée *VoIP* désigne tout trafic sans distinction. Elle est appelée dans la *policy-map* nommée *global-policy*.

Les paramètres concernant SCCP sont sous le mot `parameters`. Ceux concernant TCP sont dans la *class* nommée VoIP. Cette inspection est bien entendu applicable sur du trafic en clair mais aussi sur du trafic chiffré à condition d'avoir activé la fonction TLS-proxy.

c. Phone proxy

Cette technique est particulièrement utile pour sécuriser les réseaux au sein desquels sont présents des téléphones IP logiciel (SoftPhone). Les réseaux de téléphonie et ceux de données emploient en règle générale deux VLAN distincts. Si un téléphone logiciel est installé sur une station de travail (membre du VLAN « données ») il est alors nécessaire de faire transiter la téléphonie d'un VLAN vers l'autre ce qui soulève quelques problèmes dus à la nature des ports UDP et à leur désignation dynamique par le CUCM. Cette configuration nécessite tout comme pour le TLS-proxy l'installation de certificats sur le pare-feu afin de représenter le CUCM pour les téléphones et une mise à jour de leur liste de sécurité interne.

Le CUCM est capable d'intercepter les messages en provenance d'un téléphone logiciel du VLAN de données et de le forcer à s'authentifier. À l'issue de cette séquence la signalisation indique au pare-feu les ports par lesquels le trafic téléphonique sera autorisé à passer. Cette technique évite donc l'ouverture statique d'une trop grande plage de ports UDP.

© ENI Editions - All rigths reserved - Moha Anisa

5. VPN SSL

Les applications de type client serveur nécessitent en temps normal l'installation d'un logiciel spécifique sur la machine cliente et cela ne va pas sans poser de nombreux problèmes de déploiement et de mise à jour des versions en production. De plus, les accès distants au réseau de l'entreprise sur lesquels résident des clients spécifiques nécessitent un supplément de configuration avec l'installation des logiciels dédiés à la communication. L'avènement des applications développées pour Internet a considérablement modifié la donne en simplifiant les accès aux réseaux distants. En effet, à partir d'un simple navigateur Web il est possible d'accéder en toute sécurité à un portail sur lequel des liens redirigent l'utilisateur vers ses applications. Pour certaines d'entre elles ce mode de fonctionnement n'est pas envisageable en raison du coût de migration ou des habitudes prises par les utilisateurs. La messagerie est un exemple typique pour lequel les utilisateurs ont quelques difficultés à troquer leur traditionnel client contre une messagerie en ligne offrant pourtant les mêmes facilités. Afin de palier à cet inconvénient, il est possible de télécharger à la demande des fonctionnalités additionnelles pour canaliser ces types de trafic dans la communication protégée par SSL.

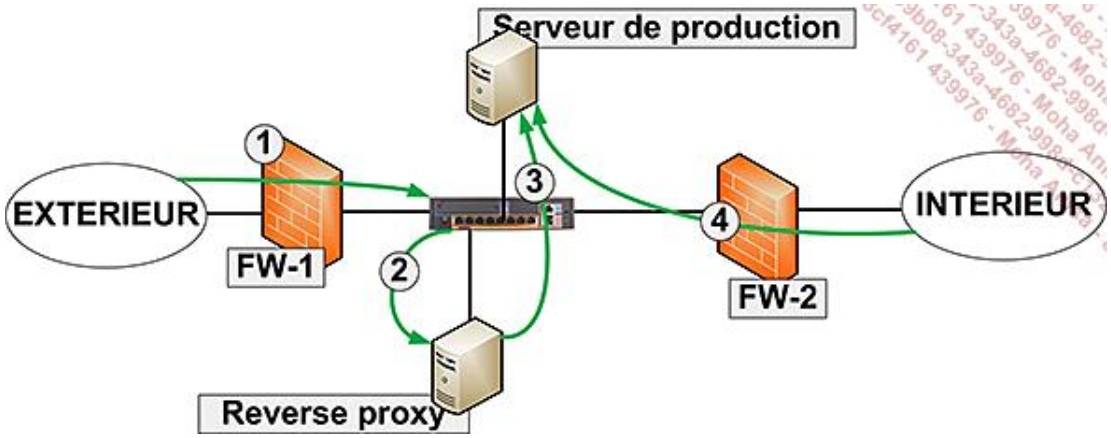
Les pare-feu Cisco ASA offrent trois techniques que nous allons examiner sous le prisme de la sécurité. Ces modes de fonctionnement sont : la connexion VPN SSL sans client, celle avec un ou plusieurs connecteurs spécifiques (plug-in) et celle avec un client lourd.

Le déploiement de cette technologie nécessite une bonne organisation afin de planifier avec soin les groupes d'utilisateurs et les droits d'accès aux ressources. Ici, la notion de groupe s'étend en fonction des projets bien au-delà des utilisateurs de l'entreprise. Ceci est du au fait que la technologie VPN SSL repousse les limites des connexions traditionnelles et offre ainsi la possibilité à une entreprise d'ouvrir ses ressources à ses partenaires sans qu'il soit nécessaire de maîtriser leur infrastructure. Un tel projet s'accompagne aussi d'une étude sur les procédures de création et de changement concernant les ressources, les groupes d'utilisateurs et les relations qui les unissent. Ces études sont, soulignons-le, étroitement liées à l'organisation des annuaires d'entreprise et plus globalement à la gestion des identités.

Cette étude comporte bien entendu (et comme toujours) une définition préalable des exigences de sécurité.

Exigences de sécurité des VPN SSL	
Authentifier les utilisateurs Leur attribuer des droits d'accès	AAA (association groupes-ressources) Gestion des mots de passe.
Valider un niveau de sécurité sur les stations distantes	Vérification de l'anti-virus, niveau minimal de chiffrement, expiration des sessions, authentification mutuelle (certificats)
Renforcer la sécurité en cas d'accès à partir de machines publiques	Secure desktop, effacement du cache, clavier virtuel, détection des enregistreurs de clavier

Ces exigences couvrent les deux domaines que sont l'équipement VPN SSL central et la station distante.



Voici une représentation très schématique d'une architecture VPN SSL sur laquelle nous observons les éléments constitutifs et les flux associés en partant du principe que l'équipement VPN SSL est en mode routé et délègue quelques fonctions de sécurité. Si tel n'est pas le cas, il s'avère indispensable d'intercaler un routeur ou un commutateur Ethernet munis de fonctions de routage. Décrivons cette architecture :

- Les stations de travail passent au travers d'un premier firewall qui a pour vocation de filtrer le protocole entrant en veillant à la bonne conformité de la couche TCP/IP et en assurant une barrière contre les attaques par saturation.

© ENI Editions - All rigths reserved - Moha Anisa

- L'équipement terminal VPN SSL termine la session chiffrée avec l'utilisateur distant et examine ses droits généralement en fonction de son groupe d'appartenance. Les annuaires de l'entreprise sont mis à contribution. Ils ne sont pas ici représentés, mais sont positionnés dans une zone de sécurité, car rappelons-le, aucun trafic externe ne doit directement accéder au réseau Interne. Ces annuaires DMZ peuvent-être des images des annuaires internes disposant d'un système de réplication de l'intérieur vers la DMZ.

- Le trafic est routé vers un équipement de type reverse-proxy afin de passer de nouveaux services de sécurité comme l'analyse des caractères dangereux avant d'être (généralement en fonction de l'URI) vers le serveur de production. Il est recommandé de chiffrer cette communication pour assurer un maximum de confidentialité au sein même des DMZ.

- Ce dernier est alimenté en donnée par l'intérieur du réseau en application du principe de moindre privilège.

Des mécanismes additionnels qui sortent du cadre de ce livre offrent la possibilité de gérer les droits d'accès en fonction de l'application demandée lors des requêtes HTTP ainsi que l'authentification unique plus connue sous l'appellation de SSO (*Single Sign On*). Toutefois certaines approches du SSO sont prises en compte par le firewall ASA.

a. VPN SSL sans client

Il s'agit du mode privilégié qui utilise les fonctions de chiffrement du navigateur Internet pour assurer la sécurité. Les clients se connectent à un portail personnalisé sur le firewall et en fonction de leur identité ont accès aux ressources pour lesquelles ils ont des droits. Il est également possible de parcourir des répertoires et des fichiers à la manière de l'explorateur d'une station de travail. Un avantage incontestable est l'accès aux données à partir de n'importe quel poste de travail reliée à Internet.

Nous allons décrire les configurations qui conduisent à la construction d'un exemple simple mettant en avant les fonctions de sécurité. Nous n'aborderons pas les multiples capacités de ce produit en matière de personnalisation des portails.

```
ASA-5505(config)# webvpn
ASA-5505(config-webvpn)# enable outside
```

Ces deux commandes activent le VPN SSL sur l'interface extérieure du firewall. Les paramètres de sécurité sont affectés à l'utilisateur une fois franchie la page d'authentification. Ils proviennent d'une combinaison des propriétés de l'utilisateur et du groupe auquel il appartient. C'est ce groupe d'appartenance qui fixe les règles de sécurité auxquelles est soumis l'utilisateur pendant sa session.

```
group-policy "Entreprise 1" internal
group-policy "Entreprise 1" attributes
 banner value Bonjour bonjour
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout 240
 vpn-tunnel-protocol webvpn
 group-lock none
 vlan none
 webvpn
  url-list value template_entreprise_1
  filter none
  port-forward disable
  customization value Entreprise_1
  hidden-shares none
  smart-tunnel disable
  file-entry enable
  file-browsing enable
  url-entry enable
  smart-tunnel auto-signon disable
username Paul password NUNxeiV/zZIW3X5z encrypted
username Paul attributes
 vpn-group-policy "Entreprise 1"
 vpn-access-hours none
 vpn-simultaneous-logins 1
 vpn-idle-timeout 30
 vpn-session-timeout 240
 vpn-filter none
 vpn-tunnel-protocol webvpn
 password-storage disable
```

© ENI Editions - All rigths reserved - Moha Anisa

```
 group-lock Entreprise_1
 service-type remote-access
 webvpn
  file-browsing enable
  file-entry enable
  url-entry enable
  port-forward disable
  homepage none
  hidden-shares none
  url-list none
  customization value Entreprise_1
  svc keep-installer installed
  svc keepalive none
  svc compression deflate
  svc dtls enable
  svc mtu 1406
  svc profiles none
  smart-tunnel disable
  smart-tunnel auto-signon disable
tunnel-group Entreprise_1 type remote-access
tunnel-group Entreprise_1 general-attributes
 default-group-policy "Entreprise 1"
 password-management password-expire-in-days 2
tunnel-group Entreprise_1 webvpn-attributes
 customization Entreprise_1
 group-alias ent1 enable
```

Voici un large extrait de la configuration d'un ASA qui montre le paramétrage d'un VPN SSL.

Cette configuration minimaliste est donnée à titre informatif et ne propose aucune fonctionnalité web, elle a pour vocation d'illustrer la manière dont l'utilisateur hérite des paramètres du VPN SSL sur lequel il se connecte. Ces paramètres viennent s'ajouter aux siens et à ceux de son groupe d'appartenance.

Les attributs de l'utilisateur Paul sont clairement visibles et notamment la politique de groupe à laquelle il est rattaché. Les paramètres de personnalisation du portail ne sont pas visibles sur la configuration car ils sont stockés dans un fichier XML lui-même sauvegardé en mémoire flash. Par commodité, cette configuration ne fait pas appel à un annuaire centralisé mais utilise la base locale AAA. Le contrôle effectué sur l'expiration du mot de passe est basé sur la lecture des propriétés venant de l'annuaire. Le firewall permet à l'utilisateur de changer lui-même son mot de passe.

Le détail de cette configuration est le suivant :

- Une politique de groupe est créée et nommée `Entreprise 1`. Elle reçoit quelques propriétés. Elles figurent sur les lignes qui sont décalées d'un caractère sur la droite.
- La commande `vpn-tunnel-protocol webvpn` appelle la commande `webvpn` située trois lignes plus bas laquelle reçoit également des propriétés (de nouveau décalées d'un caractère à droite).
- La commande `webvpn` est assortie de propriétés de personnalisation du portail comme la liste d'URL (`template_entreprise_1`).
- L'utilisateur Paul est défini et une série de caractéristiques lui sont appliquées dont son rattachement à la politique de groupe `Entreprise 1`.
- Le portail est finalement créé avec la commande `tunnel-group Entreprise_1` et reçoit la politique `Entreprise_1`.

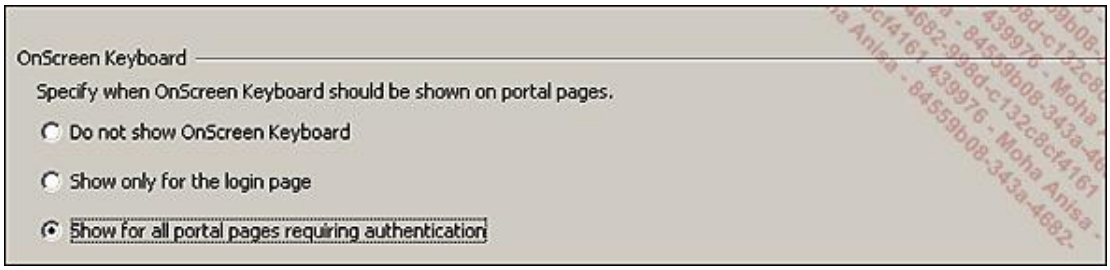
Les exigences de sécurité indiquent que la sélection des paramètres de cryptographie participe à l'évaluation du niveau de sécurité de la station distante. Les navigateurs Internet et les serveurs négocient la suite de chiffrement et en fonction de leurs possibilités s'accordent sur une suite faible.

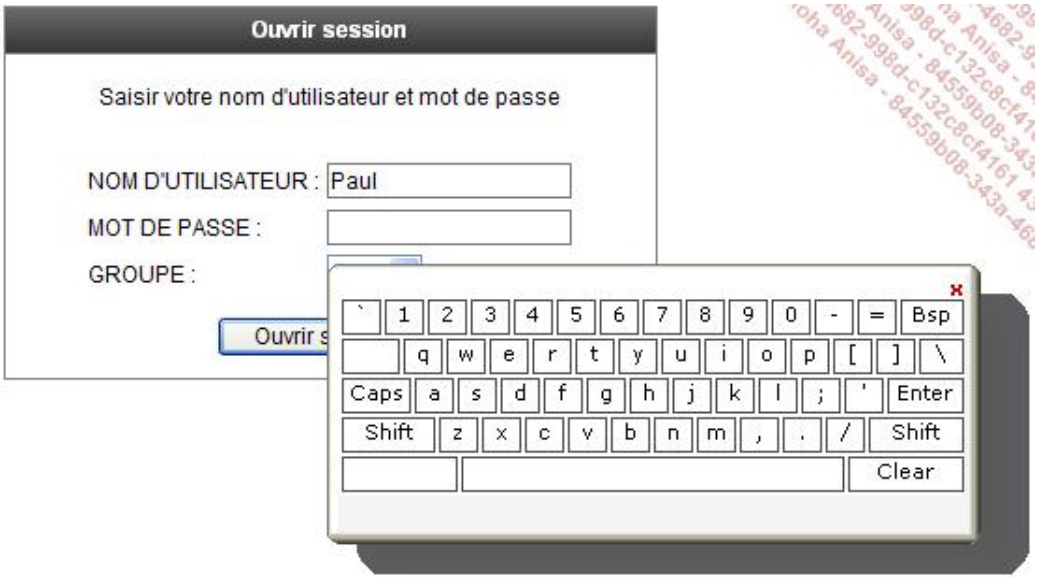
```
ASA5505(config)# ssl encryption aes256-sha1 aes128-sha1 3des-sha1
ASA5505(config)# ssl server-version tlsv1-only
```

Ces deux lignes montrent la configuration SSL du côté du firewall ASA. La négociation est acceptée pour ces trois suites et le protocole général choisi est TLS V1 ce qui signifie qu'une station distante sera rejetée si elle se présente avec une suite différente des trois proposées. L'objectif ici est de forcer la négociation sur les suites les plus fortes.

© ENI Editions - All rigths reserved - Moha Anisa

Le clavier virtuel :


OnScreen Keyboard
Specify when OnScreen Keyboard should be shown on portal pages.
Do not show OnScreen Keyboard
Show only for the login page
Show for all portal pages requiring authentication


Ouvrir session
Saisir votre nom d'utilisateur et mot de passe
NOM D'UTILISATEUR :
Paul
MOT DE PASSE :
GROUPE :
Ouvrir
` 1 2 3 4 5 6 7 8 9 0 - = Bsp
q w e r t y u i o p [ ] \
Caps a s d f g h j k l ; ' Enter
Shift z x c v b n m , . / Shift
Clear

Ces deux captures montrent le menu de configuration du clavier virtuel et le résultat obtenu lors d'une tentative d'ouverture de session. Ce dispositif protège contre les enregistreurs de clavier dont le but est de capturer les mots de passe entrés par l'utilisateur.

Secure desktop

Cisco Secure Desktop (CSD) est un environnement de travail sécurisé qui est téléchargé puis installé par un client distant. Cette technologie est souvent comparée à un bac à sable logiciel duquel on ne peut sortir. CSD est une machine virtuelle chiffrée qui une fois créée sur la station distante s'intercale entre l'utilisateur et le système d'exploitation. L'utilisateur dès lors, interagit avec ses applications à l'intérieur de cet espace virtuel local. Une fois la session terminée, l'environnement est détruit.

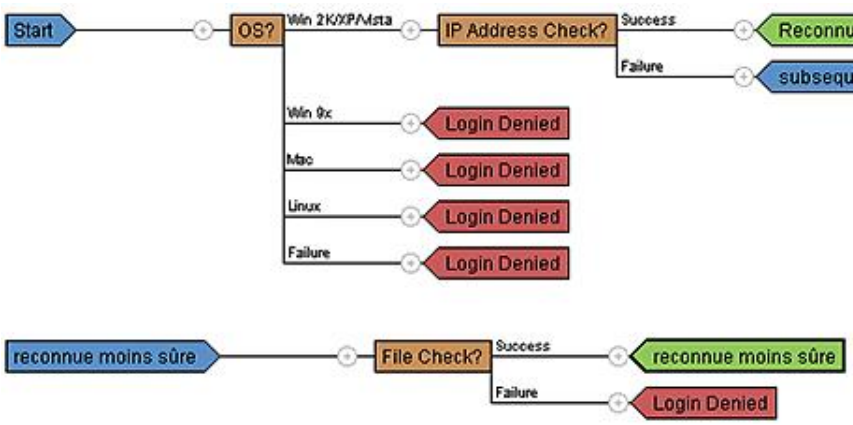
La mise en œuvre de CSD s'effectue en trois phases :

- son téléchargement sur le site de Cisco, sa copie sur le système de fichier du firewall et son activation ;
- la création d'une politique de vérification entre le moment où l'utilisateur entame la connexion et le moment où il entre ses identifiants. Le principe est de procéder à des contrôles préalables définissant un niveau de sécurité dont dépendra le type de services disponibles ou la non connexion (si le niveau minimal n'est pas atteint) ;
- La connexion proprement dite dans le client sécurisé.

```
ASA5505(config)# webvpn
ASA5505(config-webvpn)# csd image disk0:/cte/securedesktop-asa-
3.3.0.129-k9.pkg
 ASA5505(config-webvpn)# csd enable
```

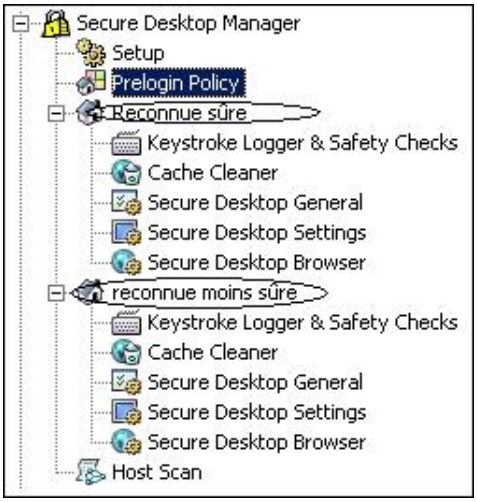
Ces trois commandes activent csd à partir d'une image logicielle préalablement téléchargée sur le site Internet de Cisco. Cette image est copiée dans un système de fichiers nommé disk 0:. La commande `csd enable` active globalement la fonction.

© ENI Editions - All rigths reserved - Moha Anisa



Ici, une fois n'est pas coutume nous présentons un extrait graphique de la configuration de la phase numéro deux. Il est ici possible graphiquement de concevoir une logique afin de classer le niveau de sécurité de la station distante en fonction de certaines de ses caractéristiques. En fonction du niveau de sécurité, CSD autorisera certaines fonctionnalités. Dans cet exemple, CSD examine le système d'exploitation de la station distante et exige la présence d'un certain type (2K/XP/Vista) avant de poursuivre par un examen de l'adresse ou du réseau IP. Si ce réseau est conforme à celui configuré dans la règle la station est reconnue sûre. La chaîne de caractère « reconnue sûre » devient de fait le nom d'une politique CSD.

La logique poursuit son cheminement en cas d'erreur sur l'adresse ou le réseau IP et la station est reconnue moins sûre. Afin de lui permettre d'accéder à un jeu réduit de fonctionnalités, cette nouvelle tentative recherche sur la station distante un fichier à un emplacement précis. S'il est trouvé, la station est affectée de l'étiquette « reconnue moins sûre » dont la chaîne de caractères devient à son tour le nom d'une politique CSD.



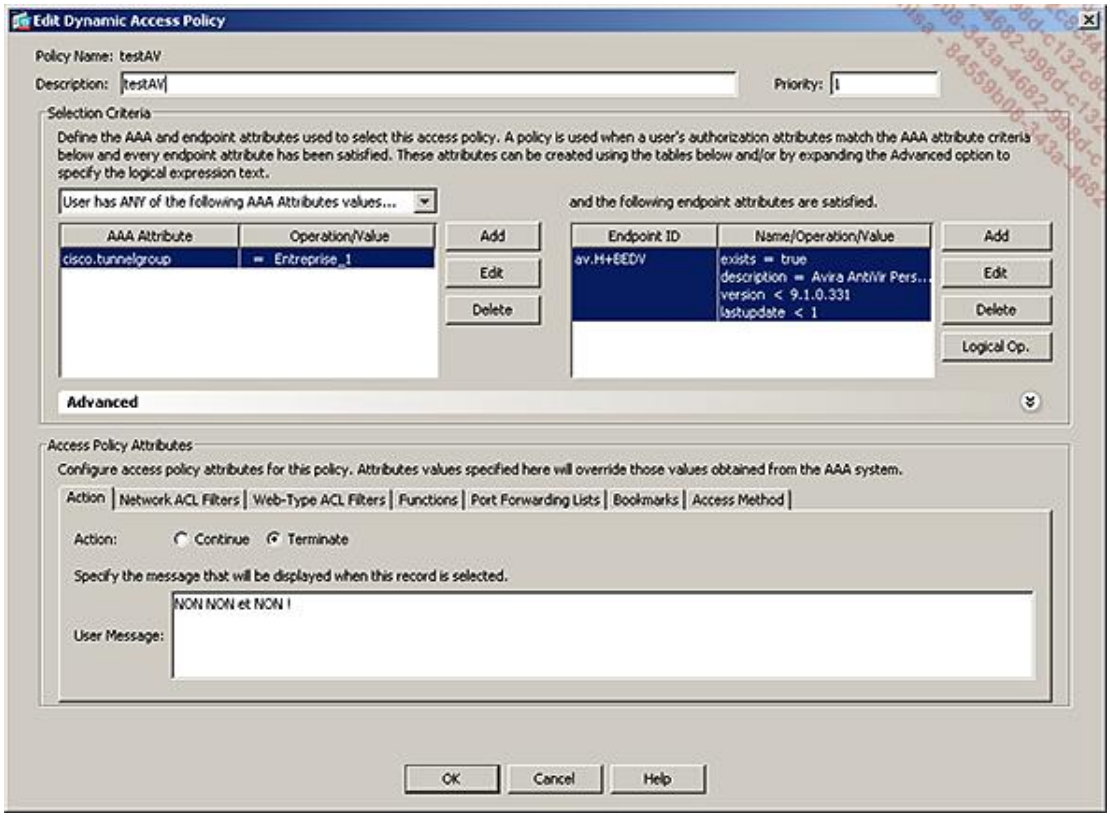
Il est possible de créer plusieurs politiques en fonction d'une analyse préliminaire de certaines caractéristiques du poste de travail. Par exemple, toute station ne possédant pas une clé spécifique dans sa base de registre est considérée comme étant dans un lieu non sécurisé. Cette politique ouvre par la suite le droit d'effectuer certaines actions comme la navigation sur Internet ou l'accès à des fichiers. L'image nous montre aussi les icônes de configuration des divers contrôles de sécurité de chaque politique. Nous y trouvons les dispositifs de nettoyage du cache de la station distante ainsi que divers autres contrôles visant à prémunir la station contre les enregistreurs de clavier ou l'introduction de médias amovibles.

© ENI Editions - All rigths reserved - Moha Anisa

Voici l'utilisateur sur le point d'entrer dans son environnement protégé par CSD. Il est indiqué qu'aucun enregistreur de clavier n'a été détecté sur la station.

Politique d'accès dynamique

Ce type de politique permet d'affecter des droits d'accès et de circulation sur le réseau à un utilisateur en fonction de ses propriétés d'authentification (AAA) et de la présence sur sa machine d'un logiciel de sécurité correctement paramétré.


Edit Dynamic Access Policy
Policy Name: testAV
Description: testAV
Priority: 1
Selection Criteria
Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.
User has ANY of the following AAA Attributes values...
and the following endpoint attributes are satisfied.
AAA Attribute
Operation/Value
cisco.tunnelgroup = Entreprise_1
Endpoint ID
Name/Operation/Value
av.M+BEDV
exists = true
description = Avira AntiVir Pers...
version < 9.1.0.331
lastupdate < 1
Add
Edit
Delete
Logical Op.
Advanced
Access Policy Attributes
Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.
Action
Network ACL Filters
Web-Type ACL Filters
Functions
Port Forwarding Lists
Bookmarks
Access Method
Action: Continue Terminate
Specify the message that will be displayed when this record is selected.
User Message:
NON NON et NON !
OK
Cancel
Help

Voici l'exemple d'une politique d'accès dynamique concernant les utilisateurs d'un profil de connexion qui doivent également satisfaire à des conditions de version d'antivirus (moteur et signature). Si l'une des conditions n'est pas remplie ou au contraire est remplie, des attributs supplémentaires sont affectés à l'utilisateur et viennent prendre le

© ENI Editions - All rigths reserved - Moha Anisa

dessus sur les valeurs obtenues par l'authentification AAA. Sur la capture d'écran, en cas de non-conformité, la connexion est coupée.

Protection applicative

L'un des objectifs de l'inspection applicative est d'examiner le contenu des paquets (filtrés par une ACL) afin de permettre au pare-feu d'ouvrir les ports nécessaires à la communication. Cette ouverture dynamique est suivie d'une fermeture des ports une fois la communication achevée. Ce principe est appliqué lors de la traversée des protocoles associées à la téléphonie sur IP.

L'inspection va aussi confronter les paquets à un groupe de règles destinées à détecter d'éventuelles irrégularités le tout donnant lieu à une décision comme dans l'exemple à suivre qui concerne HTTP et SCCP.

```
class-map Inspection_SCCP
 match any
!
class-map Inspection_HTTP
 match any
!
!
policy-map type inspect http Niveau_de_securite_HTTP
 parameters
  protocol-violation action drop-connection log
 class asdm_high_security_methods
  drop-connection
 match request header non-ascii
  drop-connection
policy-map Inspection_SCCP_et_HTTP
 class Inspection_SCCP
  inspect skinny
  set connection conn-max 100 embryonic-conn-max 20 per-client-max
100
  set connection timeout tcp 1:00:00 reset dcd 0:15:00 5
 class Inspection_HTTP
  inspect http Niveau_de_securite_HTTP
!
service-policy Inspection_SCCP_et_HTTP global
```

Nous retrouvons ici le traditionnel schéma « *class-map* dans une *policy-map* dans une *service-policy* » (cette phrase est à retenir !). Toutefois, nous observons une petite nuance. Il s'agit de la *policy-map* de type *inspect* qui est appelée dans la `policy-map Inspection_SCCP_et_HTTP`. Cette *policy-map* définit des actions en cas d'irrégularité dans le protocole. Nous sommes donc en présence d'un petit arsenal de lutte contre les attaques dissimulées dans les protocoles applicatifs.

b. VPN SSL avec Smart Tunnels

La technologie *Smart Tunnel* permet de faire transiter des applications TCP (non WEB) entre l'ordinateur distant et le site central. Smart Tunnel vient en remplacement du client léger précédent qui assurait des fonctions de redirection de port à la manière d'un client SSH. Malgré tout, il est toujours possible d'activer les fonctions de redirection de port pour les applications qui ne sont pas supportées par la technologie Smart Tunnel (Outlook MAPI).

Smart Tunnel ne nécessite pas de disposer des droits administrateur sur le poste de travail et met à disposition de l'utilisateur des connecteurs (plug-ins) pour certaines applications prédéfinies. Les connecteurs dispensent l'utilisateur de l'installation d'un programme additionnel.

```
ASA5505(config)# webvpn
ASA5505(config-webvpn)# smart-tunnel list Messagerie 1
thunderbird.exe platform windows
ASA5505(config-webvpn)# group-policy "Entreprise 1" attributes
ASA5505(config-group-policy)# webvpn
ASA5505(config-group-webvpn)# smart-tunnel enable Messagerie
```

Ici, nous configurons *Smart Tunnel* pour faire transiter le trafic issu de l'application de messagerie *thunderbird.exe* qui fonctionne sur une plate-forme Microsoft Windows.

Les connecteurs s'installent dans la mémoire flash de l'équipement via l'interface graphique après les avoir téléchargés sur le site de Cisco. Une fois en place, ils apparaissent dans le portail et donnent à l'intérieur d'une page web la possibilité de lancer une connexion SSH, RDP, Citrix ou encore VNC.

© ENI Editions - All rigths reserved - Moha Anisa

c. VPN SSL avec le client AnyConnect

Le client « lourd » *AnyConnect* s'installe manuellement ou automatiquement sur un poste client et crée sur celui-ci une interface réseau virtuelle ainsi qu'une route statique. Ce client possède un avantage certain par rapport à un client de type VPN IPSec car il est exempt de toute configuration. Une fois installé, l'utilisateur dûment authentifié est directement connecté sur le réseau local de l'entreprise. La configuration d'*AnyConnect* comporte plusieurs étapes.

```
ip local pool AnyConnect 192.168.1.10-192.168.1.20 mask
255.255.255.0
!
group-policy Client1 internal
group-policy Client1 attributes
 banner value Bonjour bonjour
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol svc
 group-lock value AnyConnect
 msie-proxy method no-proxy
 vlan none
 nac-settings none
 address-pools value AnyConnect
 webvpn
  url-list value template_entreprise_1
  svc dtls enable
  svc keep-installer installed
  svc keepalive none
  svc compression deflate
  svc profiles none
  svc ask none default svc
  customization value Entreprise_1
  deny-message value Des droits vous manquent
```

Tout d'abord, une politique de groupe est créée. Elle comporte quelques propriétés comme l'indication de la mise en place d'un tunnel SSL `vpn-tunnel-protocol svc` et l'affectation d'un groupe d'adresses IP `address-pools value AnyConnect`.

Les instructions sous `webvpn` concernent le client VPN et indiquent entre autre de laisser le programme d'installation sur la machine hôte et de forcer son installation.

```
username Paul password bI0TiI3IJ4S1atiy encrypted
username Paul attributes
 vpn-group-policy Client1
```

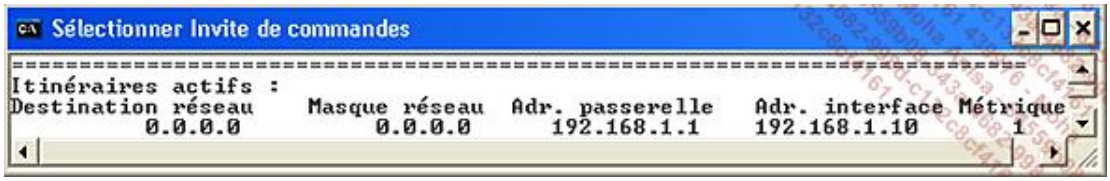
Mr Paul est rattaché à la politique de groupe précédemment créée.

```
tunnel-group AnyConnect type remote-access
tunnel-group AnyConnect general-attributes
 address-pool AnyConnect
 authentication-server-group (outside) LOCAL
 default-group-policy Client1
tunnel-group AnyConnect webvpn-attributes
 group-alias AnyC enable
```

Le tunnel est mis en place et reçoit les propriétés précédemment créées. La commande d'authentification appelle le serveur AAA interne (LOCAL) du firewall pour assurer cette fonction sur l'interface externe.

© ENI Editions - All rigths reserved - Moha Anisa

En cliquant sur le petit cadenas (première icône à gauche) nous obtenons la fenêtre qui fournit quelques indications comme l'adresse IP obtenue et celle du pare-feu sur laquelle se termine le tunnel SSLVPN.


Sélectionner Invite de commandes
Itinéraires actifs :
Destination réseau Masque réseau Adr. passerelle Adr. interface Métrique
0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.10 1

Ici, nous observons le retour de la commande `netstat -nr` sur la station de travail et nous constatons la présence d'une route par défaut pointant vers l'adresse interne du pare-feu.

```
ASA5505# sh vpn-sessiondb svc

Session Type: SVC

Username     : Paul                   Index        : 2
Assigned IP  : 192.168.1.10           Public IP    : 198.10.10.2
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : SSL VPN
Encryption   : 3DES AES256            Hashing      : SHA1
Bytes Tx     : 53140                  Bytes Rx     : 22736
Group Policy : Client1                Tunnel Group : AnyConnect
Login Time   : 18:58:50 UTC Fri Oct 24 2008
Duration     : 0h:01m:25s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Voici le résultat de la commande `show vpn-sessiondb svc` qui montre les caractéristiques de la connexion de Mr Paul. Les informations fournies sont très lisibles et directement exploitables toutefois, le mot *clientless* qui apparait ici porte à confusion.

Dans cette configuration ne figure aucune indication concernant le *split-tunneling* qui est la technique autorisant l'utilisateur d'un tunnel à en sortir pour accéder à certaines ressources. Cela signifie en l'état que ce choix n'est pas permis.

Le *split-tunneling* est utilisé pour les connexions à Internet à partir de la station de travail d'un utilisateur nomade.

© ENI Editions - All rigths reserved - Moha Anisa

En fonction de la politique de sécurité le trafic Internet de l'utilisateur nomade est soit contraint de passer par le site central ou bien autorisé à sortir directement ce qui ne va pas sans soulever quelques interrogations.

Ici, la politique de sécurité du réseau rejoint celle des stations de travail qui pour les accès nomades impose des protections comme les firewalls personnels, les antivirus et des mécanismes (ou procédures) de désactivation des interfaces autres que celle sur laquelle le tunnel est établi.

Signalons enfin qu'au niveau réseau en fonction de l'architecture les règles de traduction d'adresses devront être ajustée. La configuration présentée nécessite une règle d'exclusion car le réseau affecté à la station nomade existe sur le réseau interne.

© ENI Editions - All rigths reserved - Moha Anisa

Conclusion

Nous avons exposé dans ce chapitre quelques-unes des multiples fonctionnalités offertes par le pare-feu ASA qui vont bien au-delà de la simple confrontation du trafic à des règles de filtrage. Sans cette évolution, ce type de matériel serait sans doute tombé en désuétude. Le pare-feu ASA de Cisco est un équipement multifonction aux possibilités remarquables qui reprend les fonctions de base comme le filtrage et y ajoute celles issues des boîtiers VPN. Toutes les couches du modèle OSI sont couvertes et les protocoles applicatifs bénéficient d'un puissant service d'analyse permettant de parer aux problèmes d'irrégularités et d'attaques embarquées.

Le VPN SSL est une avancée significative permettant aux entreprises de fournir des accès applicatifs en toute sécurité à leurs partenaires avec ou sans l'installation d'un client spécifique. Ces accès sont également subordonnés à des contrôles de sécurité sur le poste client portant sur le type de système d'exploitation ou d'antivirus.

Le pare-feu ASA vient également au service de la téléphonie sur IP avec une prise en compte des spécificités de ses protocoles parmi lesquelles figurent l'attribution dynamique des ports de communication.

Dans l'architecture de sécurité, le pare-feu de Cisco occupe, de par ses capacités d'analyse multicouches, des positions qui ne se limitent pas aux frontières avec le monde extérieur car ses spécificités font de lui un appareil capable de protéger également l'intérieur du réseau.

© ENI Editions - All rigths reserved - Moha Anisa

Virtualisation (VMware)

Ce livre a grandement bénéficié de l'essor des technologies de virtualisation et d'émulation. Nous allons dans ce chapitre décrire les méthodes qui nous ont permis de réaliser les maquettes destinées à concevoir et à valider les configurations présentées dans ce livre. Deux logiciels particulièrement performants ont été mis à contribution. Nous citerons en premier l'incontournable *VMware* puis le couple *Dynamips*, *GNS3*.

La virtualisation consiste à utiliser un système d'exploitation afin de faire fonctionner en son sein d'autres systèmes d'exploitation. La virtualisation est apparue pour le grand public à la fin des années 90 avec l'avènement du logiciel *VMware*. Elle possède à son actif de nombreux avantages parmi lesquels nous pouvons citer une réduction du nombre de machines présentes dans les salles informatiques grâce aux regroupements effectués sur des machines hôtes. Outre le gain de place évident, la virtualisation simplifie la création et le déplacement de systèmes d'exploitation virtuels entre les machines hôtes diminuant ainsi les coûts associés à l'exploitation.

La *virtualisation* présente d'indéniables avantages en ce qui concerne la création de réseaux à des fins d'essais lors de phases d'intégration et de validation d'un projet informatique. Il est en effet facile de créer, de modifier, de déplacer et de supprimer un système d'exploitation virtuel. Un autre avantage est de pouvoir aisément déplacer un groupe de machines virtuelles dans le cadre de démonstrations car elles prennent la forme d'un ensemble de quelques fichiers. La capture d'écran montre une machine hôte Microsoft Windows Vista hébergeant une machine virtuelle Linux. L'hôte fournissant le service d'hébergement est également désigné par l'appellation d'*hyperviseur*. Les machines virtuelles avec certaines versions de VMware (ACE) peuvent être chiffrées et recevoir des politiques de sécurité. VMware est aussi présenté sous une forme qui constitue elle-même un système d'exploitation. Il s'agit de la version ESX qui s'installe directement sur le matériel. Il n'est plus indispensable d'installer un système d'exploitation hôte comme Microsoft Windows (ce qui est le cas sur la capture d'écran).

La virtualisation d'un système Linux permet de bénéficier de tous les services réseaux offerts par les distributions. Nous avons pour la préparation de ce livre utilisé VMware pour installer sur notre machine hôte un serveur Linux FEDORA sur lequel nous avons installé le serveur FreeRADIUS.

Les réseaux et VMware

Une machine virtuelle est utilisable en circuit fermé. Cette configuration est utile pour découvrir le système Linux (ou un autre) sans avoir à l'installer à demeure et de manière isolée. Toutefois, une machine virtuelle peut se connecter à la machine hôte et au réseau de celle-ci. La version que nous avons utilisée propose trois modes de fonctionnement qui consistent à :

- Connecter la machine virtuelle uniquement à la machine hôte. Il s'agit du mode *host Only* disponible généralement sur l'interface VMNet1. La machine virtuelle se voit attribuer une adresse IP par le serveur DHCP de Vmware. Ce mode de fonctionnement permet à la machine virtuelle de dialoguer uniquement avec la machine hôte.

- Connecter la machine virtuelle au monde extérieur via la machine hôte. Pour ce faire cette dernière opère une traduction d'adresse. Il s'agit du mode NAT disponible sur l'interface VMNet8.

© ENI Editions - All rigths reserved - Moha Anisa

- Connecter la machine virtuelle aux côtés de son hôte sur le même réseau. Il s'agit du mode *bridged* pour lequel la machine virtuelle possède sa propre adresse IP comme n'importe quelle autre machine sur du réseau local.

Cette image illustre notre description : http://sebsauvage.net/temp/ccm/types_reseau_vmware.png

---

Installation du produit

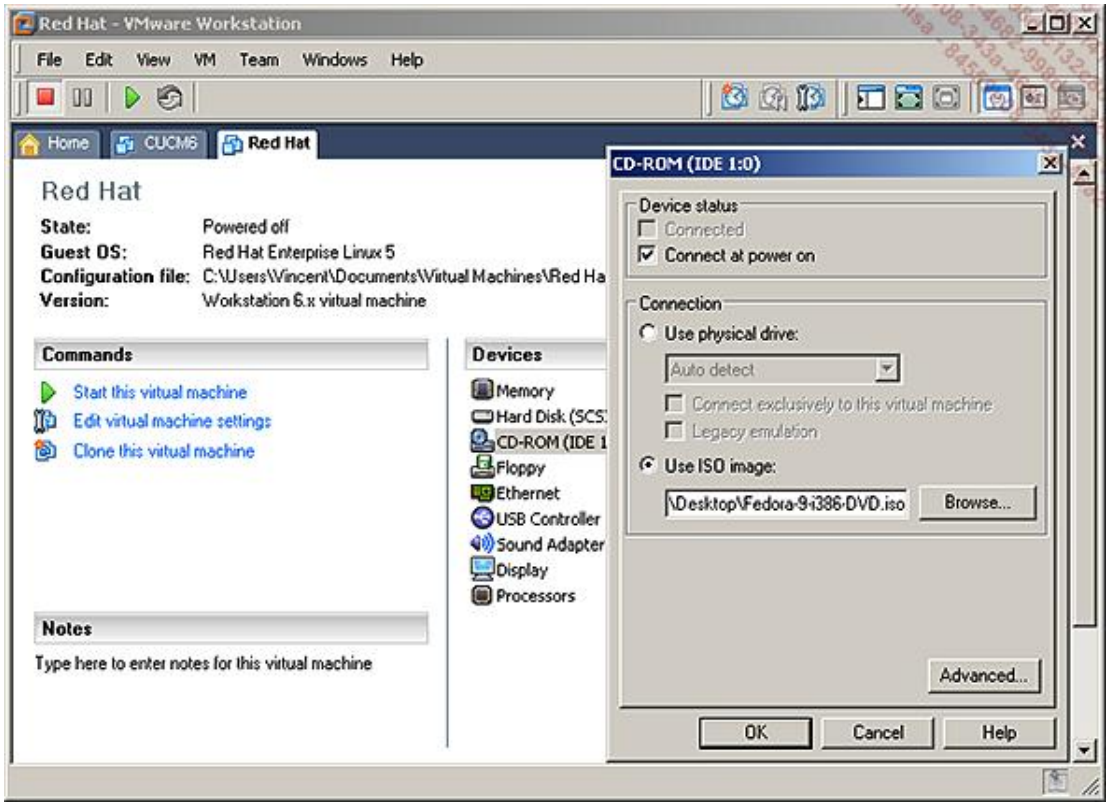
L'installation d'une machine virtuelle est relativement simple. Pour installer un système Linux, il est recommandé de se procurer une image ISO qui est habituellement utilisée pour graver un CD ou un DVD du système.

Pour créer une nouvelle machine virtuelle, il suffit de suivre les étapes suivantes :

- Sélectionner **File** puis **New** puis **Virtual Machine** et suivre l'assistant. Ce dernier propose plusieurs choix de systèmes d'exploitation ainsi que l'espace disque réservé à la machine virtuelle sur le système hôte.

- Sélectionner le CD-Rom et choisir d'utiliser une image ISO.

- Cliquer sur le triangle vert pour lancer l'installation du système qui se déroule comme lorsqu'un ordinateur est mis en route et se lance avec un disque dans le lecteur de CD-Rom.



Cette capture d'écran montre l'étape durant laquelle l'image ISO du système *Linux Fedora* est sélectionnée pour l'installation.

© ENI Editions - All rigths reserved - Moha Anisa

Émulation

Nous avons également fait usage de la technique d'émulation pour simuler un réseau de routeurs Cisco. La frontière est mince entre l'émulation et ce que nous venons de décrire avec la virtualisation. Ici, l'ordinateur va simuler l'électronique du routeur afin de faire fonctionner le logiciel IOS. Cette technique d'émulation est très utilisée dans le monde du développement sur microprocesseur. Nous la retrouvons aussi dans un autre domaine qui se trouve être celui de l'univers des jeux vidéos des années 80. Ces jeux d'arcade ont en effet trouvé une seconde jeunesse grâce aux multiples émulateurs qui pour notre plus grand bonheur ressuscitent des jeux comme le célèbre *Pacman*.

Dynamips et GNS3

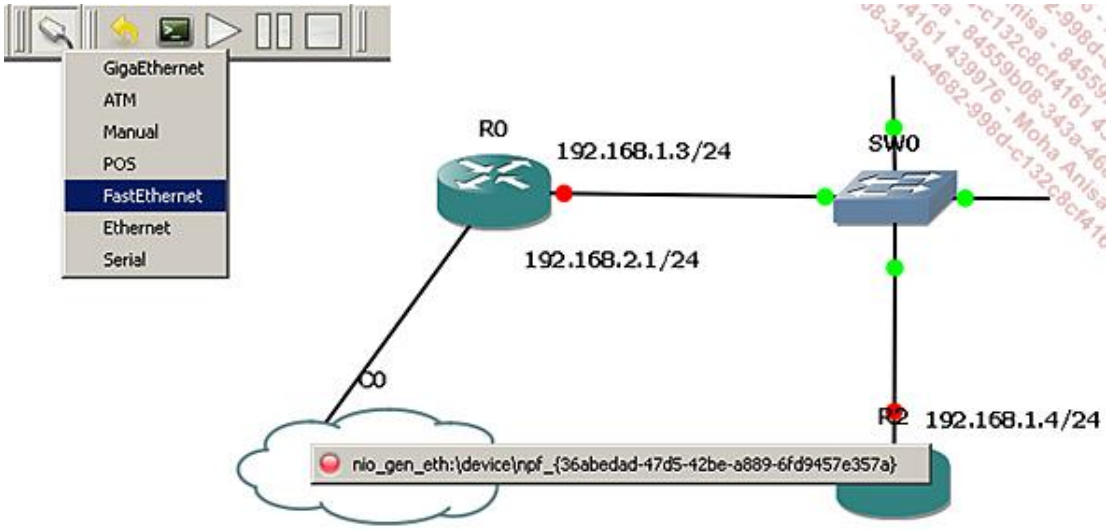
Ces deux logiciels sont indissociables et permettent d'émuler un routeur Cisco sans son système d'exploitation. Les diverses plate-formes qu'il est possible d'émuler sont les suivantes : C1700, C2600, C2691, C3600, C3700, C7200.

Il est important de préciser que le système d'exploitation IOS est sous licence. Pour utiliser *Dynamips*, il est donc indispensable de posséder légalement une image système. *Dynamips* reçoit donc une image système compatible avec la plate-forme choisie ainsi qu'un fichier de configuration qui comporte le paramétrage des interfaces et des interconnexions avec les autres routeurs et même la carte réseau de l'hôte local. *Dynamips* se configure aussi avec une interface graphique nommée GNS3.

Installation du produit

Le logiciel est disponible pour Windows et MacOs X. Le code source est également proposé sur le site Internet www.gns3.net. Le téléchargement pour Windows comprend tous les éléments additionnels requis. Parmi eux figure l'interface de programmation (API) PCAP bien connue des utilisateurs du logiciel Wireshark (ex Ethereal) qui permet de capturer le trafic sur un réseau Ethernet non commuté.

Après l'installation qui est des plus classique, le logiciel montre sur une colonne plusieurs icônes représentant chacune un modèle de routeurs, de commutateur Ethernet, frame-relay, ATM ainsi que le pare-feu PIX. En sélectionnant le menu **edit** puis **IOS images et hypervisors** on obtient la fenêtre qui permet de renseigner la version d'IOS qui sera utilisée par la suite.



En faisant glisser les icônes de la colonne de gauche vers le centre de l'interface graphique et en reliant les icônes entre elles comme le montre la capture d'écran, nous créons une petite architecture sur laquelle apparaissent deux routeurs, un commutateur Ethernet et un nuage. Les liaisons se dessinent après avoir sélectionné l'icône représentant une souris, il convient alors de tracer les liaisons entre les divers équipements. Lorsque le pointeur se trouve au dessus de l'objet à connecter, une petite fenêtre apparait et permet de sélectionner l'interface de destination.

Le nuage est un objet à part entière. Il est utilisé pour relier la maquette à la carte réseau de l'ordinateur hôte afin de la rendre disponible à distance et de la connecter à divers services comme des annuaires, des enregistreurs de journaux (Syslog) ou des serveurs d'authentification.

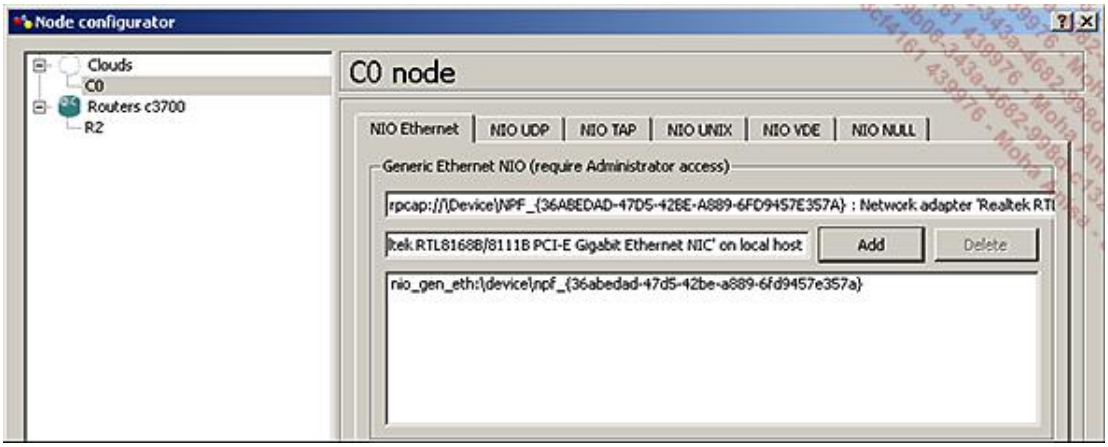
Lorsque toutes les étapes menant à la réalisation de la maquette sont terminées, il est recommandé de sauvegarder la configuration. Le fichier de configuration pour Dynamips est alors créé.

```
[localhost]

    [[7200]]
    image = \Program Files\Dynamips\images\c7200-jk9o3s-mz.
124-7a.image
    # On Linux / Unix use forward slashes:
```

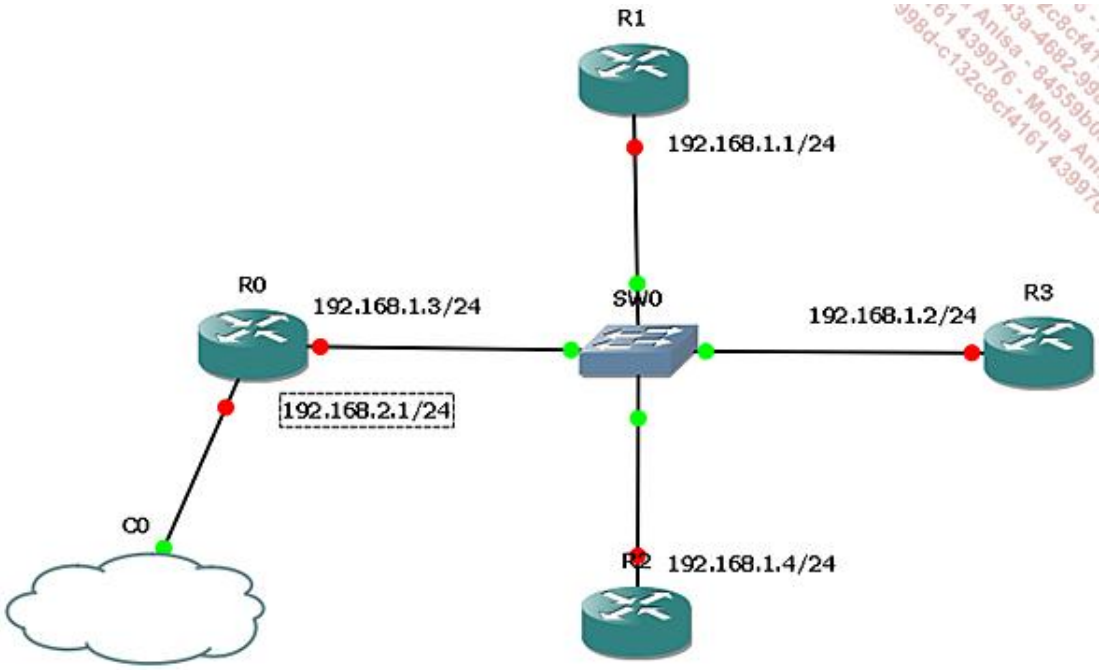
© ENI Editions - All rigths reserved - Moha Anisa

```
    #image = /opt/7200-images/c7200-ik9o3s-mz.124-5a.image
    npe = npe-400
    ram = 160

    [[ROUTER R1]]
    F1/0 = S1 1

    [[ethsw S1]]
    1 = access 1
    2 = access 20
    3 = dot1q 1
    # Note, replace the interface below with a valid interface
    # on your system or Dynamips will crash!
    #4 = dot1q 1 NIO_gen_eth:eth0
    4 = dot1q 1 NIO_gen_eth:\Device\NPF_{B00A38DD-F10B-43B4-99F4-
B4A078484487}
```

Voici un exemple de configuration de Dynamips. Nous observons l'image IOS choisie pour les routeurs de la maquette. Chaque routeur fait l'objet d'une déclaration sur laquelle figurent ses connexions vers les autres objets de la maquette. Ici, le routeur R1 est connecté par son interface F1/0 (pour *Fast Ethernet* 1/0) au port numéro 1 du commutateur S1 ce dernier étant représenté par l'entrée ethsw S1 qui comporte 3 interfaces. Les interfaces numéro 1 et 2 sont chacune dans un VLAN (1 et 20), quant à l'interface 3 elle est reliée à un *trunk* de type dot1q lui-même connecté à une carte réseau de la machine hôte.



Voici le détail de la configuration du nuage vu par l'interface graphique. Une liste déroulante montre toutes les interfaces de la machine hôte éligibles pour servir de connexion entre la maquette et la machine hôte.



Voici une maquette comprenant quatre routeurs reliés entre eux par un commutateur Ethernet. Le routeur R0 est

© ENI Editions - All rigths reserved - Moha Anisa

connecté à la carte réseau de la machine hôte en passant par le nuage C0 (Cloud 0).

© ENI Editions - All rigths reserved - Moha Anisa

Conclusion

Les avantages des produits comme *VMware* ou *Dynamips*, *GNS3* sont multiples, mais le revers de la médaille est une augmentation considérable des ressources (mémoire et processeur) qui sont consommées par ces programmes sur le système hôte. Il devient possible dans un environnement réduit à une seule machine de mettre en œuvre une maquette réseau et système très complète et relativement complexe. Ces techniques permettent aisément de sauvegarder les diverses configurations et de les installer à loisir. Les techniques de virtualisation et d'émulation sont en quelque sorte respectueuses de l'environnement en permettant de réaliser des économies d'électricité et d'espace, c'est pour ces raisons qu'elles connaissent depuis quelques années déjà un franc succès.

© ENI Editions - All rigths reserved - Moha Anisa

Conclusion

Cisco depuis 1985 propose des solutions pour les réseaux et a su dès le commencement de son activité associer à ses produits des fonctions de sécurité innovantes. Nous avons largement utilisé au cours de ce livre les fameuses ACL qui au-delà de leur rôle en matière de sécurité sont employées chaque fois qu'une sélection de trafic s'avère nécessaire. Dès lors, Cisco a entamé une série d'acquisition de société dont certaines ont apporté leur savoir-faire dans le domaine de la sécurité. Ce fut le cas pour le pare-feu phare de la marque dont nous avons étudié le successeur. De même, chaque diversification dans la gamme de produit fut systématiquement accompagnée d'innovations visant à protéger les fonctions de routage, de commutation ou plus récemment de voix sur IP.

Nous n'avons pas été exhaustifs dans ce livre car nous avons eu la volonté de traiter le vaste sujet que représente la sécurité avec Cisco sous le prisme des équipements les plus couramment rencontrés dans les petites et moyennes entreprises. Bien d'autres solutions et technologies sont disponibles au catalogue comme les sondes de détections d'intrusion, la protection de la messagerie ou les dispositifs d'accès au réseau (NAC). Malgré tout, nous avons indirectement abordé quelques-uns de ces sujets notamment au cours du chapitre sur la sécurité de la couche logique.

L'approche matérielle et technologique n'est pourtant pas suffisante pour assurer pleinement la mission consistant à protéger un réseau et les applications qui l'empruntent. Avec l'accroissement des menaces et la diversification des matériels, les équipements seuls ne suffisent pas à accomplir la tâche qui leur est confiée sans une solide organisation. C'est pourquoi, avant toute chose, il est primordial de mener à bien une réflexion structurée auprès des utilisateurs du réseau afin de connaître et donc de comprendre leurs besoins sécuritaires et les risques associés à la perte ou à l'indisponibilité du réseau.

Des équations complexes alliant la multiplication de la variable risque à la division par la variable menace sont disponibles un peu partout et les longs rapports d'analyse de risques basés sur d'improbables hypothèses de départ versent parfois dans le catastrophisme le plus pathétique. Dans le domaine de la sécurité, toutes les informations sont recevables et les décisions doivent être prises en dehors de toute peur ou affolement savamment entretenu par les marchands de solutions miracles qui ne manquent pas de se presser aux portes des entreprises. Une analyse pragmatique accompagnée de bon sens valent souvent bien mieux que certaines études bien éloignées de la réalité de l'entreprise. La phase d'étude et de réflexion est d'autant plus importante que le prix des équipements de sécurité est relativement élevé et leur implémentation complexe.

Le principal acteur de la sécurité trop souvent oublié est l'utilisateur. Les architectures, les systèmes et les réseaux sont tous au service des utilisateurs. Il peut arriver que ce facteur humain soit négligé ou tout bonnement écarté. Pourtant, aucune politique de sécurité n'est totalement opérationnelle sans l'adhésion totale et sans réserve des utilisateurs. Ici et là, se développent des campagnes de sensibilisation parfois fort coûteuses sur le bien-fondé de la sécurité informatique et son lien étroit avec la santé économique de l'entreprise. Hélas, ces tentatives qui restent trop souvent vaines conduisent irrémédiablement les responsables à durcir les règles au grand mécontentement de tous.

Nous l'observons fréquemment dans la presse, les affaires impliquant la sécurité informatique se multiplient et la part de plus en plus importante qu'occupe l'économie numérique dans le monde incite les criminels en systèmes d'information à déployer toujours plus d'ingéniosité pour s'emparer d'informations sensibles ou d'argent. Face à cette menace, la sécurité des réseaux et des données qui y transitent devient une préoccupation pour tous les acteurs de cette économie à commencer par les usagers eux-mêmes.

Ce livre consacré à la sécurité des réseaux avec les solutions de Cisco se veut avant tout une ouverture vers l'ensemble des approches matérielles et conceptuelles dans ce passionnant domaine qui n'a pas fini de faire parler de lui.

© ENI Editions - All rigths reserved - Moha Anisa